锐捷 NBR 系列路由器
用户手册

V1.0

版权声明

前言

版本说明

本手册适用于锐捷 NBR 系列 NBR100 路由器。

内容介绍

这份手册主要介绍了锐捷 NBR 系列路由器的硬件特性、安装配置维护以及常见故障的排除。

在安装路由器之前及安装过程中为避免可能出现的设备损坏和人身伤害，请仔细阅读本手册。

📖 **建议：**

建议由熟悉电气环境、线缆连接以及有实际安装和配置路由器经验的专业技术人员进行安装和配置。

这份手册包括以下章节：(以下的章节目录不对)

-

介绍了锐捷 NBR 系列路由器的外观图以及系统特性；

-

描述了安装路由器的环境要求、安装前和安装过程中需要注意的事项、安装所需工具。

-

介绍路由器的机械安装方法、电源连接方法、备份口电缆连接方法以及配置口电缆连接方法；

-

介绍如何启动并对路由器进行基本的配置。

-

介绍了如何处理安装过程中可能出现的问题以及各种 LED 的含义；

-

介绍了如何对路由器进行主体软件、BOOTROM 软件进行升级；

感谢您选择锐捷 NBR 系列路由器！

说明：

该安装手册只介绍如何安装锐捷 NBR 系列路由器,要使用路由器还需要进行具体的配置，关于如何配置路由器的详细信息，请参考相关部分的配置参考。

在本手册中，锐捷 RG-NBRxxx 系列路由器简称为锐捷 NBRxxx 系列路由器。

详细的说明和配置以随机附带的光盘为准，如果因为时间而有改变，恕不另行通知。

读者对象

本书适合下列人员阅读

- **网络工程师**
- **技术推广人员**
- **网络管理员**

本书约定

1、通用格式约定

宋体：正文采用 5 号宋体。

楷体：警告、说明等提示等内容一律用楷体，并且在内容前后增加线条与正文隔离。

`Terminal Display` 格式：自定义的 `Terminal Display` 格式，英文 `Courier New` ，中文宋体，文字大小 `8.5` ，表示屏幕输出信息此外屏幕输出。信息中夹杂的用户从终端输入的信息，采用**加粗字体**表示。

2、各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标

志的意义如下：

⚡： 警告、危险、提醒操作中应注意的事项。

ⓘ： 小心、注意、提醒操作中应注意的事项。

🕮： 说明、提示、窍门、对操作内容的描述进行必要的补充和说明。

目　录

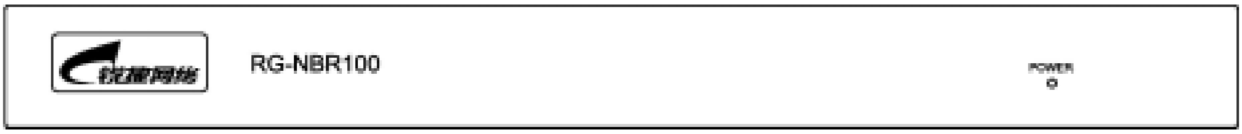
第一章 产品介绍

锐捷 NBR 系列路由器，是利用国际先进的半导体技术及通讯控制技术，由锐捷网络有限公司自主开发的数据通讯产品，具有自主知识产权。锐捷路由器完全按照国际标准进行开发，无论在使用方式及配置方法上都与目前国际流行的主流路由器产品相似，已经熟悉主流路由器配置命令的网络管理员通过阅读本手册，可不经培训直接配置使用本产品。

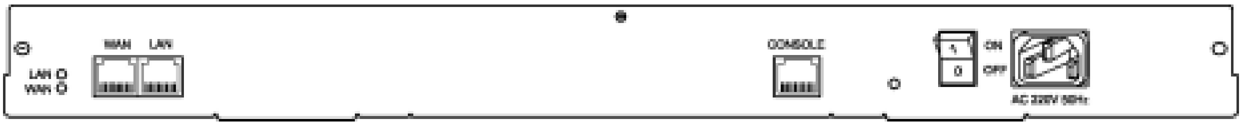
1.1 锐捷 NBR 系列路由器

1.1.1 锐捷 NBR100 路由器

1.1.1.1 锐捷 NBR100 路由器外观图



锐捷 NBR100 路由器前面板



锐捷 NBR100 路由器后面板

1.1.1.2 锐捷 NBR100 路由器基本配置

锐捷 NBR100 的基本配置如下：

项目	描述
内存	DRAM：16MB
	FLASH：8MB
	BOOTROM：512K
I/O 设置	WAN 口：1 个 10/100M 自适应以太网口，可以自动识别网线和交叉线。 LAN 口：1 个 10/100M 自适应快速以太网口，可以自动识别网线和交叉线。
	控制台口：1 个

接口标准	以太网：10Base-T/100Base-T
	配置口（控制台口）：RS-232
外型尺寸(高×长×宽)	44.4mm×444.5mm×268.2mm
电压	AC: 170~264V 47/63Hz
功率	小于 30W
工作环境	温度：0~40℃
	湿度：10~90% 不结露

说明：

动态存储器 DRAM 作为主存储器，即内存。

FLASH 储存主体软件。

NVRAM 储存开机配置文件（startup-config）。

1.2 锐捷路由器特点

1.2.1 丰富的协议支持

锐捷系列路由器适用于众多的网络环境

- 提供双绞线 RJ45 接口，支持以太网协议、ARP 协议
- 网络层上支持 TCP/IP 协议簇，实现了 IP、ICMP、IGMP、TCP 和 UDP、DNS 等协议
- 支持多种 IP 上的动态路由协议：RIP（V1/V2）,策略路由等
- 支持网络管理协议 SNMP
- 支持 TELNET
- 支持反向 TELNET
- 支持 DHCP Server、DHCP Client、DHCP Relay 等
- 支持 PPPOE
- 支持 DNS 静态域名解析
- 支持异步文件传输协议 X-MODEM、Y-MODEM 升级方式
- 支持 NAT
- 支持 TFTP

1.2.2 友好的用户界面

- 提供标准操作界面，配置直观，每条命令均提供详细的在线帮助。
- 使用手册中针对各条命令都有详细的说明和示例，并提供全面的故障分析描述。

1.2.3 丰富的诊断和管理工具

- 提供了完备的调试跟踪手段，提供了丰富的 DEBUG 指令，方便准确的定位各种网络故障。
- 提供了丰富的统计和状态信息显示功能，使用户对网络的性能和运行状态一目了然。
- 支持多种终端登录配置方式：
    - 通过 Console 口进行配置
    - 通过 TELNET 登录配置
    - 通过 TFTP 服务器配置

1.2.4 良好的安全性

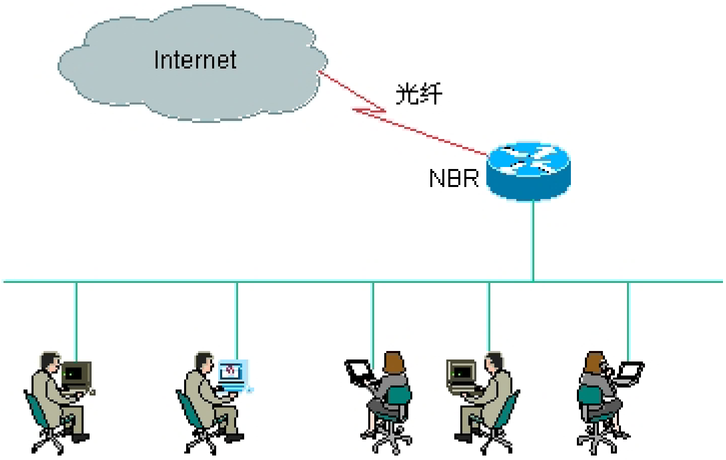
- 采用完善的防火墙和 IP 包过滤技术，对网络地址、端口号或协议类型均可进行严密检查。
- PPP 协议上实现了 PAP 和 CHAP 协议。
- 支持 MAC 地址绑定功能。
- 网络地址翻译技术 NAT

1.2.5 方便的升级途径

- 支持异步文件传输 X-MODEM、Y-MODEM 协议，可以在各种操作环境(如 Windows 95、Windows NT、UNIX、DOS 等)下通过 Console 口或同步口下载新的升级版本。
- 可以支持通过 TFTP 协议下载新的软件版本。
- 支持 BOOTROM 在线升级。

1.3 典型应用

网吧、小型企业、家庭使用锐捷 NBR 系列路由器接光纤宽带上网，拓扑图如下：



其中 NBR 通过光纤转换器使用光纤与 Internet 连接。

第二章 路由器安装前的准备

2.1 安全注意事项

路由器承担着网络连接的中转站的重要作用，其正常使用关系到整个网络是否能正常运作。

在路由器的安装和使用过程中特提出如下的安全建议

- 请不要将路由器放置在有水的地方，也不要让液体进入路由器。
- 请将路由器放置在远离热源的地方。
- 请确认路由器的正常接地。
- 请用户在安装维护过程中佩戴防静电手腕。
- 请不要带电插拔路由器的模块。
- 请不要带电插拔电缆。
- 不要穿着松散的服装以防勾住器件造成损坏，为此请系紧衣带、围巾，扎好衣袖。
- 将工具、器件放在远离人员行走的地方以防碰。
- 建议用户使用 UPS 不间断电源，一方面可以避免断电，另一方面可以避免电源干扰。

2.2 安装环境要求

锐捷系列路由器必须在室内使用，为保证路由器正常工作和延长使用寿命。安装场所应该满足下列要求：

- 温度/湿度要求
- 洁净度要求
- 防静电要求
- 抗干扰要求
- 防雷击要求
- 检查安装台

2.2.1 温度/湿度要求

为保证路由器正常工作并延长其使用寿命，机房必须维持一定的温度和湿度。若机房长期湿度过高，则易造成绝缘材料绝缘不良甚至发生漏电现象等机械性能变化现象；若相对湿度过低，则绝缘垫片可能会干缩而引起紧固螺丝松动，在干燥的气候环境下容易产生静电，危害路由器上的内部电路。温度过高会加速绝缘材料的老化过程，使路由器的可靠性大大降低，严重影响其使用寿命。

锐捷系列路由器对温度湿度的要求见下表：

温度		相对湿度	
长期工作条件	短期工作条件	长期工作条件	短期工作条件
15℃~30℃	0℃~40℃	40%~65%	10%~90%

说明：

工作环境温度湿度是指在路由器机架前后没有保护板时距地板以上 1.5m 和距路由器架前方 0.4m 处测量所得的数值。

短期工作条件指路由器连续工作不超过 48 小时或每年累计不超过 15 天。

极端恶劣工作环境一般指路由器机房内空调系统出现故障，每次不应超过 5 小时即能恢复正常工作范围时可能出现的环境温度和湿度值。

2.2.2 洁净度要求

灰尘对路由器的运行安全也是一大危害，室内灰尘落在路由器上会造成静电吸附，导致接触不良，不但影响设备寿命，而且容易造成通信故障。当室内相对湿度偏低时，更易产生这种静电吸附。

锐捷系列路由器对机房内的灰尘含量及粒径要求见下表：

最大直径(μm)	0.5	1	3	5
最大浓度(每立方米所含颗粒数)	1.4×10^{7}	7×10^{5}	2.4×10^{5}	1.3×10^{5}

除灰尘外，路由器对机房空气中所含的盐酸硫化物也有严格的要求，这些有害气体会加速金属的腐蚀和某些路由器部件老化过程，机房内对 SO_2、H_2S、NO_2、NH_3、Cl_2 等有害气体的具体限制值见下表：

气体	平均（mg/m^3）	最大（mg/m^3）
SO_2	0.2	1.5
H_2S	0	0.03
NO_2	0.04	0.15
NH_3	0.05	0.15
Cl_2	0.01	0.3

2.2.3 防静电要求

路由器在设计电路时已作了防静电处理，但过强的静电仍会对路由器电路板产生破坏。与路由器连接的通信网中静电主要来自以下两个方面：

- 室外高压输电线、雷电等外界电场环境。
- 室内环境地板材料整机结构等内部系统。

因此，为防止静电的破坏应做到：

- 设备及地板良好接地
- 室内防尘
- 保持适当的温度湿度
- 接触路由器电路板时，应戴防静电手腕穿防静电工作服。
- 将拆卸下的路由器电路板面朝上放置在抗静电的工作台上或放入电磁屏蔽袋中。
- 观察或转移拆卸的路由器电路板时，请用手接触电路板的外边缘避免用手直接触摸电路板上的元器件。

2.2.4 抗干扰要求

这里抗干扰只要是指电磁、电流等干扰，下面是抗干扰的一些要求：

- 对供电系统采取有效的防电网干扰措施。
- 路由器工作地最好不要与电力设备的接地装置或防雷接地装置合用并尽可能相距远一些。
- 远离强功率无线电发射台、雷达发射台等高频大电流设备。
- 必要时采取电磁屏蔽的方法。

2.2.5 防雷击要求

锐捷系列路由器对防雷击作了处理，但是作为一种电气设备，过强的雷击仍可能对其造成损坏。所以，采取防雷击措施是必须的：

- 保证路由器接地线与大地保持良好接触。
- 保证交流电源插座的中性点与大地良好接触。
- 为了增强电源的防雷击效果，可以考虑在电源的输入前端加入电源避雷器。

2.2.6 检查安装装置

无论将路由器安装在机柜内还是直接放在工作台上，都需要保证以下条件：

- 确认路由器的入风口及通风口处留有空间以利于路由器机箱的散热。锐捷系列路由器自身配有散热风扇，其散热原理是：从机壳四周的散热孔抽进冷空气，通过风扇从机壳下方排出。因此在散热孔的周围，至少留有 10mm

的空间，确保有足够的散热空间。建议将路由器安装在 19"标准机柜上。在没有条件的地方，也可以将路由器水平放置在干净的平面上。在较炎热的地区，建议安装空调。

- 确认机柜和工作台自身有良好的通风散热系统。
- 确认机柜及工作台足够牢固，能够支撑路由器及其安装附件的重量。
- 确认机柜及工作台的良好接地。

2.3 安装工具和设备

为了您的安装顺利，请准备：

- **安装工具**
- **连接电缆**
- **相关设备**

安装工具包括：

- 十字螺丝刀
- 一字螺丝刀
- 防静电手腕

连接电缆包括：

- 电源线
- 配置线
- 以太网线
-

📖 **说明：**

锐捷系列路由器随机附电源线、配置线、网线以及相关接头，如果还需要其他的线缆，需要用户自己另外采购。

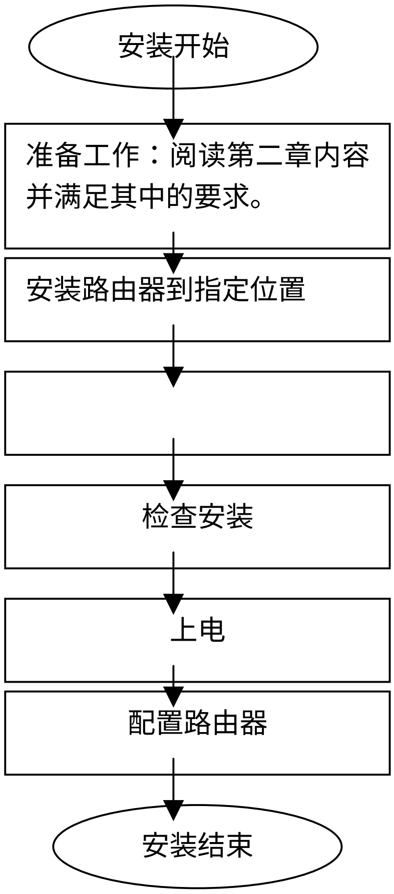
相关设备包括：

- HUB 或交换机
- 配置终端可以是终端，也可以是一台安装有超级终端的 PC 机
-
- 电源插座

第三章 路由器的安装

3.1　路由器的安装流程

为了避免在安装过程中出现手忙脚乱或者误操作导致路由器损坏，请按照一下流程进行安装：



3.2　固定路由器位置

安装路由器到指定位置即固定路由器，在安装准备工作结束以后，接着需要把路由器固定到指定位置。路由器的安装位置一般只有以下两种情况：

- 安装到机柜上
- 安装在工作台上

3.2.1 安装到机柜上

锐捷系列路由器是按照 19 英寸标准机柜的尺寸进行设计的，您可以根据机柜的情况使用路由器随机带的固定附件进行安装。

3.2.2 安装在工作台上

由于经济等各种原因，很多情况下用户并不具备 19 英寸标准机柜，更经常是将路由器放置在干净的工作台上，此种操作比较简单，操作中需要注意如下事项：

- 保证工作台的平稳性与良好接地。
- 使用随机带的塑料垫粘到路由器底部的小孔上，同时在路由器周围留出 10cm 的散热空间。
- 不要在路由器上面放置重物。

3.3 安装电源线及地线

锐捷系列路由器支持以下交流电源：

AC: 170~264V 47/63Hz

请确认您的电源满足要求。

路由器的电源线是三线的，建议使用有中性点接头的单相三线电源插座或多功能微机电源插座，电源的中性点在建筑物中要可靠接地。一般楼房在施工布线时已将本楼供电系统的电源中性点埋地，您需要确认本楼电源是否已经正确接地。

请按照以下步骤安装电源线：

第一步，确认路由器电源开关置于“ 关 ”位置后，将路由器随机所带的电源线一端插到路由器机箱后面板上的电源插座上，另一端插到交流电源插座上。

第二步，把路由器电源开关拨到“ 开 ”位置。

第三步，检查路由器前面板电源灯是否变亮，灯亮则表示电源连接正确。

3.4 连接控制台

锐捷系列路由器提供了一个符合 EIA/TIA-232 异步串行规范的配置口 Console，通过这个接口用户可完成对路由器的本地配置。

配置属性：

参数	说明
接头	RJ-45
接口标准	异步 EIA/TIA-232
波特率	300-115200bps，默认是 9600bps。
支持服务	1、命令行接口 2、与字符终端相连 3、当作一个异步接口，提供终端接入服务。

您可以通过以下步骤连接路由器控制台口：

第一步，使用随机附带的 DB-9 或 DB-25 孔式插头接到要对路由器进行配置的微机或终端的串口上。如果是微机，请确认微机上有超级终端。

第二步，使用随机附带配置线，一端连到路由器的控制台口，另一端连接 DB-9 或 DB-25 插头的 RJ45 接口。

3.5 安装后的检查

路由器机械安装完成后，在路由器上电启动前请先进行如下检查：

- 若路由器安装在机柜上，请检查机柜与路由器的安装角铁是否牢固；若安装在工作台上，请检查路由器周围是否留有足够的散热空间，工作台是否稳固。
- 检查电源线所接电源与路由器要求电源是否一致。
- 检查路由器的地线是否连接正确。
- 检查路由器与配置终端等其它设备的连接关系是否正确。

第四章 快速配置指导

这一章将给出 NBR 功能快速配置说明，其中通过几个典型应用示例的配置过程来说明，用户可以对照自己的应用模式进行类比配置。如果用户需要更进一步的配置，请参考 NBR 功能高级配置部分的说明。无论是 NBR 功能的快速配置还是 NBR 功能的高级配置，都必须首先启动路由器并搭建配置环境。

4.1　启动路由器

4.1.1 搭建配置环境

在路由器第一次使用的时候，必须采用通过 Console 口方式对路由器进行配置，具体的操作步骤如下：

第一步：如图 4-1 所示，将一字符终端或者微机的串口通过标准的 RS232 电缆和路由器的 Console 口（也叫配置口或控制台口）连接。

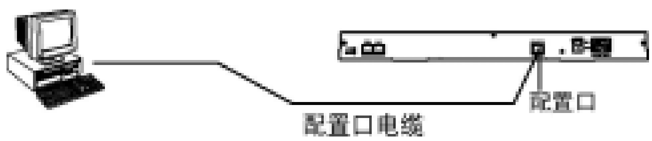


图 4-1 通过 Console 口搭建本地配置环境

第二步：配置终端的通讯设置参数，如果采用微机，则需要运行终端仿真程序，如 Windows 操作系统提供的 Hyperterm(超级终端)等，以下以超级终端为例，说明具体的操作过程。运行超级终端软件，建立新连接，选择和路由器的 Console 连接的串口，设置通讯参数：9600 波特率、8 位数据位、1 位停止位、无校验、无流控，并且选择终端仿真类型位 VT100，如下图的 Windows 的超级终端的设置界面。



图 4-2 建立新连接



图 4-3 选择和路由器的 Console 连接的微机串口

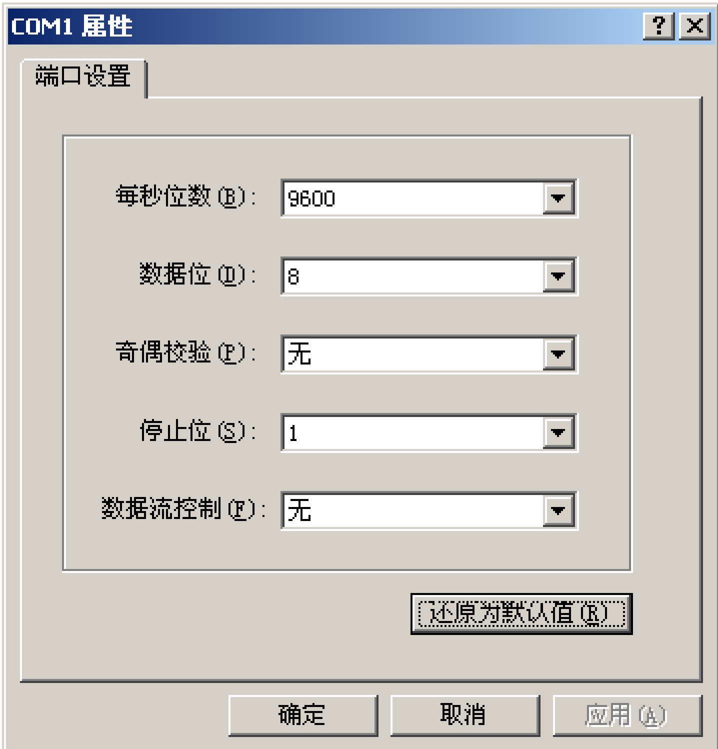


图 4-4 设置串口的通讯参数

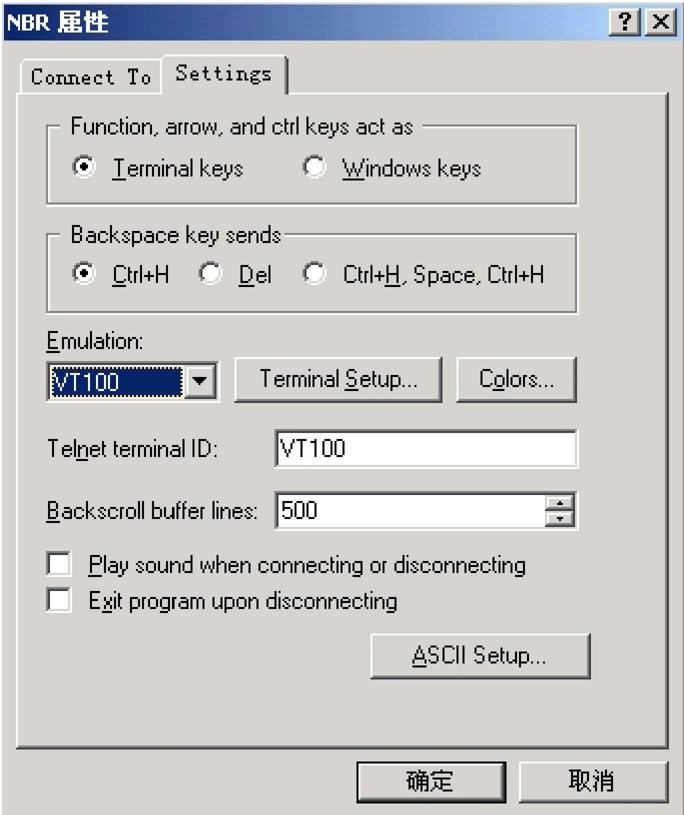


图 4-5 选择终端仿真类型

搭建完配置环境，即可对路由器进行上电。

4.1.2 路由器上电

4.1.2.1 上电前检查

在上电之前，请对路由器进行如下检查：

- 电源线和地线连接是否正确
- 供电电压与路由器的要求是否一致
- 配置电缆连接是否正确配置用微机或终端是否已经打开并设置完毕

警告：

请在路由器上电之前，确认路由器供电开关的位置，以便在发生事故时能够及时切断供电电源。

4.1.2.2 路由器上电

- 打开路由器供电电源开关

- 打开路由器电源开关，将路由器电源开关置于“ 开 ”位置

4.1.2.3 上电后检查

路由器上电后，请进行如下检查：

- 通风系统是否正常

检查方法：路由器上电后应该可以听到风扇旋转的声音，把手放在路由器的通风孔附近应该可以感觉到空气的流动。

- 路由器前面板上的指示灯显示是否正常

检查方法：路由器上电后，前面板上的 POWER 指示灯常亮。

- 配置终端是否显示正常

检查方法：路由器上电后终端上会显示路由器软件自解压等信息，同时提示是否接入 setup 配置过程。

4.1.3 启动过程

路由器第一次启动，会出现如下信息：

```
Start BOOTROM V1.9

Sizing CPU RAM...
Found 16MB CPU RAM...
Verifying
checksum ......#######################################################
##########################################################################
######
#####################################[0x6ecf][OK!]
Now Loading Image......
##########################################################################
######
##########################################################################
######
###########
Image load complete! Please wait ...

Uncompress begin...
Uncompressing the image :
========================================================== [OK]

Red-Giant Operating System Software
RGNOS (tm) RELEASE SOFTWARE, Version 6.13(3)
Copyright (c) 1999-2003 by Start Network Technolgy co., Ltd.
Compiled 2003-03-20 16:27

SUMSUNG K9F6408 ,Flash ID=ECE6
Start Red-Giant NBR100 series NBR100
Samsung 4530(ARM7TDMI) processor with 14336K/2048K bytes of memory.
Processor board ID 00000062, with hardware revision 00000002
Controllers/Moduler cards list:

Samsung 4530 10/100M ethernet controller.
-----------------------------------------------
```

```
2 FastEthernet/IEEE 802.3 interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Notice: NVRAM invalid, possibly due to write erase.
       --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes]:
```

如果您对路由器配置很熟悉，可以按 no 退出 setup 配置模式，进入用户 EXEC 模式。

建议：

第一次使用路由器，我们建议使用 NBR100 提供的针对网吧的 setup 配置功能对路由器一些基本参数进行设置。

4.1.4 通过 Setup 配置路由器

路由器第一次启动，会出现是否进入 setup 配置模式提示。您可以输入'*yes*'或者'y'进入 setup 智能配置模式，对路由器的基本参数进行配置，也可以键入'*no*'或者'n'退出自动配置模式，进入高级配置模式，进行配置。

Setup 配置参数说明如下：

```
Start BOOTROM V1.9 build 1 for NBR
Verifying
checksum ......#######################################################
####################################################################[0x91e
2][OK!
]
Now Loading Image......
##########################################################################
######
###########################################
Image load complete! Please wait ...

Uncompress begin...
Uncompressing the image : ========================================== [OK]

Red-Giant Operating System Software
RGNOS (tm) RELEASE SOFTWARE, Version 6.13(3nbr)
Copyright (c) 1999-2004 by Start Network Technolgy co., Ltd.
Compiled 2004-01-09 11:10

SUMSUNG K9F6408 ,Flash ID=ECE6
Start Red-Giant NBR100 series NBR100
Samsung 4530(ARM7TDMI) processor with 14336K/2048K bytes of memory.
```

```
Processor board ID 000000B1, with hardware revision 00000001
Red-Giant SC4530(ARM7TDMI) NBR100 platform.
Controllers/Moduler cards list:

Samsung 4530 10/100M ethernet controller.
-----------------------------------------------
2 FastEthernet/IEEE 802.3 interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Notice: NVRAM invalid, possibly due to write erase.
        ------------ 交互式系统配置 ----------------

输入 ctrl-c 中止配置流程；默认配置参数在'[]'中。
是否进入初始配置流程? [yes]: yes            <= 选择是否进入初始配置流程

配置全局参数:                               <= 配置路由器的名称
  请输入路由器名称（只能用字母数字组合） [Red-Giant]: NBR

Enable secret 是一个单向的加密密钥,它优先于 enable password 被采用
  请输入 enable secret: private             <= 配置进入特权用户层的密码

Enable password 在没有配置 enable secret,
或者在使用旧的软件版本以及某些 boot 映象软件时被采用
  请输入 enable password: puzzle   <=配置进入特权用户层的密码,优先级低于 secret
  请输入虚拟终端登陆密码: remoteuser <=配置允许远程用户 Telnet 登陆时的口令

启动防止冲击波病毒功能会降低性能，如果没有病毒，可以不启动
是否启动此功能? [no]: no            <=关闭冲击波病毒防护功能


请选择上网模式:                     <=选择 WAN 口接入 Internet 的模式
       1. 固定 IP 地址
       2. PPPOE 连接
       3. DHCP 分配 IP
请输入数字 1---3: 1

配置广域网口 FastEthernet0:          <=在当前模式下配置 WAN 口 IP 地址以掩码
  请输入 IP 地址: 218.6.92.21
  请输入地址掩码 [255.255.255.0]:

是否允许 ping 广域网接口? [yes]:     <=允许应答来自广域网上的针对广域网口的 Ping

配置局域网口 FastEthernet1:          <=在当前模式下配置本地局域网的地址
  请输入 IP 地址: 192.168.0.1
  请输入地址掩码 [255.255.255.0]:

配置默认网关:                        <=配置广域网口的下一跳路由信息
       请输入默认网关 IP 地址:218.6.92.1

是否对内部局域网启用 DHCP SERVER 功能? [no]: no    <=关闭 DHCP Server 功能

配置完毕，生成的配置脚本文件如下:     <=预览配置脚本

hostname NBR
ip routing
```

```
enable secret 5 $1$aBgm$QujUHlPDifkjVHBfX21hE1
enable password puzzle
line vty 0 4
password remoteuser
!
!
interface FastEthernet0
no shutdown
ip address 218.6.92.21 255.255.255.0
ip nat outside
!
!
interface FastEthernet1
no shutdown
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0  218.6.92.1
!
ip nat inside source list 1 interface FastEthernet 0 overload
ip nat optimize
!
access-list 1 permit any
!
end

是否应用此配置? [yes/no]: yes        <=保存并应用当前设置
Building configuration...
在 enabled 模式下使用'configure'命令可修改这些配置。


Press RETURN to get started!


NBR>
NBR>enable                          <=进入特权用户层
Password:                           <=输入设定的特权用户口令
NBR#
```

建议：

Setup 配置模式通常用于路由器首次上电时，对路由器进行引导配置，也可以在特权用户模式下随时执行特权用户模式命令 *setup* 命令进入 *setup* 配置模式。以上的配置的提示信息只是一个示例，具体应用的时候请以当前 RGNOS 以及随机附带的 CD-ROM 上的说明为准。

4.2　配置路由器

要使用路由器，必须根据需要对路由器进行具体的配置，下面将结合典型的应用使用具体的示例来将描述如何在 NBR 上配置 IP 地址、静态路由、防火墙、PPPoE、

DHCP 以及 NAT，其中使用'!"开头的斜体蓝色部分是注释说明，不是配置。如果用户需要了解更详细的功能配置，可以参考下一章相关的功能配置说明部分。

说明：

下面的典型配置示例均是基于以下这种情况，即不进入初始配置流程，而是借助自动配置命令 *setup* 来实现。

4.2.1 固定 IP 地址接入典型配置

如图 4-6，用户使用电信的光纤线路接入 Internet，用户将电信提供的光纤接头通过光纤转换器与路由器的 WAN 口连接。用户在 WAN 口上使用电信分配的广域网地址 218.5.19.2，在 LAN 口上使用内部网地址 192.168.0.1，该地址即内部网关地址。用户在 LAN 和 WAN 口上配置了 NAT 以使内部网用户可以共享光纤线路来访问 Internet。

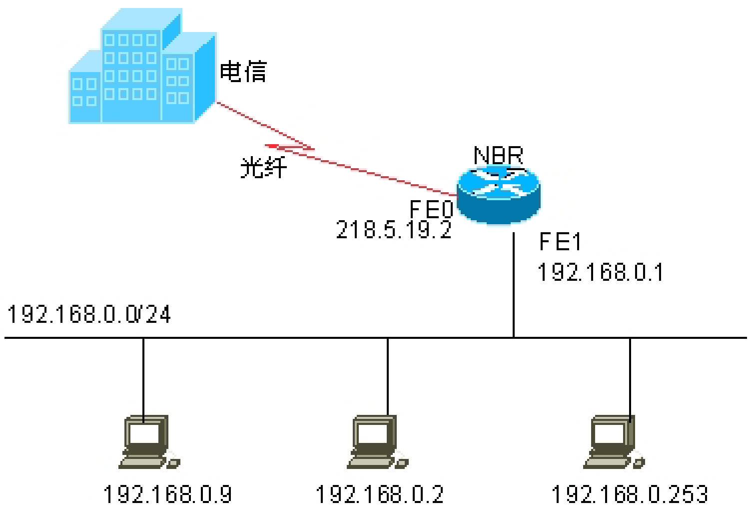


图 4-6 固定 IP 地址接入典型配置示例

在这种情况下，就可以在 NBR 上如下配置即可：

Red-Giant>**enable**
!启动快速配置功能
Red-Giant#**setup**
　　　　------------ 交互式系统配置 ----------------
输入 ctrl-c 中止配置流程；默认配置参数在'[]'中。
!选择是否进入快速配置流程
确定进入交互式系统配置? [yes]: **yes**
配置全局参数:
　请输入路由器名称（只能用字母数字组合） [Red-Giant]: **NBR**
!配置进入特权用户层的口令,这里 secret 与 password 同为进入用户层的口令，不过 secret 的安全性和优先级高于 password。
Enable secret 是一个单向的图形加密密钥,它优先于 enable password 被采用
　请输入 enable secret: **private**
Enable password 在没有配置 enable secret,

或者在使用旧的软件版本以及某些 boot 映象软件时被采用
  请输入 enable password: **puzzle**
!配置允许远程 Telnet 登陆的用户密码
  请输入虚拟终端登陆密码: **remoteuser**
!启动防止冲击波病毒的功能
启动防止冲击波病毒功能会降低性能，如果没有病毒，可以不启动
是否启动此功能? [no]: **yes**
!选择广域网接入方式。这个示例中由于是通过电信的光纤接入，广域网使用的是电信分配的固定 IP 地址，故这里选择模式 1
请选择上网模式:
    1. 固定 IP 地址
    2. PPPOE 连接
    3. DHCP 分配 IP

请输入数字 1---3: **1**
!这里为广域网接口 FastEthernet 0 设置电信分配的固定 IP 地址以及掩码。
配置广域网口 FastEthernet0:
  请输入 IP 地址: **218.5.19.2**
  请输入地址掩码 [255.255.255.0]:

!禁止广域网上其他用户 ping 广域网口以防止来自广域网上的 Ping 攻击。
是否允许 ping 广域网接口? [yes]: **no**
!配置本地局域网口 FastEthernet 1 的地址和掩码，这也是内部网关的地址
配置局域网口 FastEthernet1:
  请输入 IP 地址: **192.168.0.1**
  请输入地址掩码 [255.255.255.0]:
!配置广域网路由信息,这里设置的是广域网下一跳路由。
配置默认网关:
    请输入默认网关 IP 地址:**218.5.19.1**
!内部网络的网络主机使用的是固定 IP 地址，因此无需为内部主机开启 DHCP Server 功能。
是否对内部局域网启用 DHCP SERVER 功能? [no]:
!至此，快速配置生成的配置教本预览
配置完毕，生成的配置脚本文件如下:

```
hostname NBR
ip routing
enable secret 5 $1$I3u0$.RIU6kH0S.fil.ivOe9td1
enable password puzzle
line vty 0 4
password remoteuser
!
!
interface FastEthernet0
no shutdown
ip address 218.5.19.2 255.255.255.0
ip access-group 100 in
ip nat outside
no ip unreachables
!
!
interface FastEthernet1
no shutdown
ip address 192.168.0.1 255.255.255.0
ip access-group 100 in
ip nat inside
!
```

```
access-list 100 deny icmp any any echo
access-list 100 deny icmp any any echo-reply
ip route 0.0.0.0 0.0.0.0  218.5.19.1
!
ip nat inside source list 1 interface FastEthernet 0 overload
ip nat optimize
!
access-list 1 permit any
access-list 100 deny tcp any any eq 135
access-list 100 deny tcp any any eq 136
access-list 100 deny tcp any any eq 137
access-list 100 deny tcp any any eq 138
access-list 100 deny tcp any any eq 139
access-list 100 deny tcp any any eq 445
access-list 100 deny udp any any eq 135
access-list 100 deny udp any any eq 136
access-list 100 deny udp any any eq netbios-ns
access-list 100 deny udp any any eq netbios-dgm
access-list 100 deny udp any any eq 139
access-list 100 deny udp any any eq 445
access-list 100 deny tcp any any eq 4444
access-list 100 deny udp any any eq tftp
access-list 100 permit ip any any
access-list 100 deny icmp any any echo
access-list 100 deny icmp any any echo-reply
!
end
```

!确定保存当前配置

```
是否应用此配置? [yes/no]: yes
Building configuration...
[OK]
在 enabled 模式下使用'configure'命令可修改这些配置。

NBR#
%UPDOWN: Line protocol on Interface FastEthernet0, changed state to up
%UPDOWN: Line protocol on Interface FastEthernet1, changed state to up
%CHANGED: Interface Dialer0, changed state to administratively down
%UPDOWN: Interface FastEthernet0, changed state to up
%UPDOWN: Interface FastEthernet1, changed state to up
```

!再次检查配置.

```
NBR#show running-config
Building configuration...

Current configuration:
!
!
hostname "NBR"
!
enable secret 5 $1$I3u0$.RIU6kH0S.fil.ivOe9td1
enable password puzzle
!
!
!
ip subnet-zero
!
interface FastEthernet0
 ip address 218.5.19.2 255.255.255.0
 ip access-group 100 in
 no ip unreachables
```

```
 ip nat outside
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip access-group 100 in
 ip nat inside
!
ip nat inside source list 1 interface FastEthernet0 overload
ip nat optimize
ip classless
ip route 0.0.0.0 0.0.0.0 218.5.19.1
access-list 1 permit any
access-list 100 deny  icmp any any echo
access-list 100 deny  icmp any any echo-reply
access-list 100 deny  tcp any any eq 135
access-list 100 deny  tcp any any eq 136
access-list 100 deny  tcp any any eq 137
access-list 100 deny  tcp any any eq 138
access-list 100 deny  tcp any any eq 139
access-list 100 deny  tcp any any eq 445
access-list 100 deny  udp any any eq 135
access-list 100 deny  udp any any eq 136
access-list 100 deny  udp any any eq netbios-ns
access-list 100 deny  udp any any eq netbios-dgm
access-list 100 deny  udp any any eq 139
access-list 100 deny  udp any any eq 445
access-list 100 deny  tcp any any eq 4444
access-list 100 deny  udp any any eq tftp
access-list 100 permit ip any any
!
line con 0
line vty 0 4
 password remoteuser
 login
!
end
```

4.2.2 PPPoE 接入典型配置

如图 4-7,用户使用 ADSL 线路接入 Internet,用户使用以太网线将 ADSL Modem(此时 ADSL Modem 处于桥接模式)的 RJ-45 接口与路由器的 WAN 口连接起来。用户在 WAN 口上使用配置 PPPoE，WAN 口的 IP 地址由 PPPoE 协商得到，在 LAN 口上使用内部网地址 192.168.0.1，该地址即内部网关地址。用户在路由器上配置了 NAT 以使内部网用户可以共享光纤线路来访问 Internet。

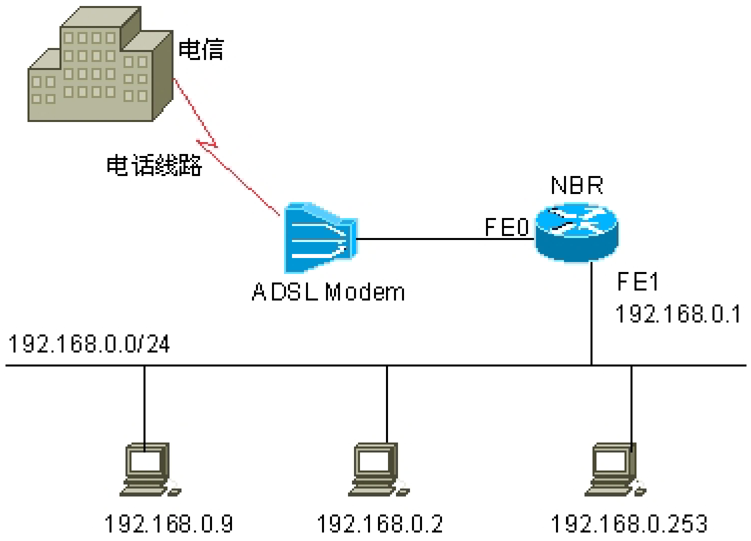


图 4-7 PPPoE 接入典型配置示例

在这种情况下，就可以在 NBR 上如下配置即可：

!进入特权用户层
Red-Giant>**enable**
!启动快速配置功能
Red-Giant#**setup**
　　　------------ 交互式系统配置 ---------------
输入 ctrl-c 中止配置流程；默认配置参数在'[]'中。
!再次确认是否进行快速配置
确定进入交互式系统配置? [yes]: **yes**
配置全局参数:
!配置路由器名称
　请输入路由器名称（只能用字母数字组合） [Red-Giant]: **NBR**
!配置进入特权用户层的口令,这里 secret 与 password 同为进入用户层的口令，不过 secret 的安全性和优先级高于 password。
Enable secret 是一个单向的图形加密密钥,它优先于 enable password 被采用
　请输入 enable secret: **private**
Enable password 在没有配置 enable secret,
或者在使用旧的软件版本以及某些 boot 映象软件时被采用
　请输入 enable password: **puzzle**
!配置允许远程 Telnet 登陆的用户密码
　请输入虚拟终端登陆密码: **remoteuser**
!启动冲击波病毒防护功能。如果确认内部网没有感染冲击波病毒，建议不要启动该防护功能以免降低系统性能。
启动防止冲击波病毒功能会降低性能，如果没有病毒，可以不启动
是否启动此功能? [no]: **yes**
!选择上网模式即 WAN 口接入 Internet 的模式,这里使用的是 PPPoE 模式。
请选择上网模式:
　　　1. 固定 IP 地址
　　　2. PPPOE 连接
　　　3. DHCP 分配 IP
请输入数字 1---3: **2**
!设置局域网口地址即本地网关地址以及 IP MTU
配置局域网口 FastEthernet1:
　请输入 IP 地址: **192.168.0.1**
　请输入地址掩码 [255.255.255.0]:

请输入 MTU [1488]:
!设置 PPPoE 工作参数
配置 PPPOE 参数:
请输入用户名: **pppoeusername**
请输入密码: **pppoepassword**
请输入 MTU [1488]:
!由于内部网主机的 IP 地址是静态配置的，这里就无需启用 DHCP Server 功能
是否对内部局域网启用 DHCP SERVER 功能? [no]:
!预览通过快速配置生产的配置脚本文件
配置完毕，生成的配置脚本文件如下:

```
hostname NBR
ip routing
enable secret 5 $1$U8e1$ai/JCzDmSJwi9dwu/z9fr0
enable password puzzle
line vty 0 4
password remoteuser
!
!
interface FastEthernet0
no shutdown
no ip address
pppoe enable
pppoe-client dial-pool-number 1 dial-on-demand
!
!
interface FastEthernet1
no shutdown
ip address 192.168.0.1 255.255.255.0
ip access-group 100 in
ip nat inside
ip mtu 1488
!
interface Dialer0
ip address negotiate
encapsulation ppp
dialer pool 1
dialer-group 1
dialer idle-time 200
ppp pap sent-username pppoeusername password 0 pppoepassword
mtu 1488
ip access-group 100 in
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 Dialer 0
!
ip nat inside source list 1 interface Dialer 0 overload
ip nat optimize
!
access-list 1 permit any
access-list 100 deny tcp any any eq 135
access-list 100 deny tcp any any eq 136
access-list 100 deny tcp any any eq 137
access-list 100 deny tcp any any eq 138
access-list 100 deny tcp any any eq 139
access-list 100 deny tcp any any eq 445
access-list 100 deny udp any any eq 135
access-list 100 deny udp any any eq 136
```

```
access-list 100 deny udp any any eq netbios-ns
access-list 100 deny udp any any eq netbios-dgm
access-list 100 deny udp any any eq 139
access-list 100 deny udp any any eq 445
access-list 100 deny tcp any any eq 4444
access-list 100 deny udp any any eq tftp
access-list 100 permit ip any any
dialer-list 1 protocol ip permit
!
end
```

!选择保存并应用这份配置

```
是否应用此配置? [yes/no]: yes
Building configuration...
[OK]
%UPDOWN: Line protocol on Interface FastEthernet0, changed state to up
%UPDOWN: Line protocol on Interface FastEthernet1, changed state to up
在 enabled 模式下使用'configure'命令可修改这些配置。

NBR#
%UPDOWN: Interface FastEthernet0, changed state to up
%UPDOWN: Interface FastEthernet1, changed state to up
```

!再次确认配置

```
NBR#show running-config
Building configuration...

Current configuration:
!
!
hostname "NBR"
!
enable secret 5 $1$U8e1$ai/JCzDmSJwi9dwu/z9fr0
enable password puzzle
!
!
!
ip subnet-zero
!
interface FastEthernet0
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1 dial-on-demand
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip access-group 100 in
 ip mtu 1488
 ip nat inside
!
interface Dialer0
 mtu 1488
 ip address negotiate
 ip access-group 100 in
 encapsulation ppp
 ip nat outside
 dialer pool 1
 dialer idle-timeout 200
 dialer-group 1
 ppp pap sent-username pppoeusername password 7 12371502450831133 83F124A132D
```

```
!
ip nat inside source list 1 interface Dialer0 overload
ip nat optimize
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
access-list 1 permit any
access-list 100 deny   tcp any any eq 135
access-list 100 deny   tcp any any eq 136
access-list 100 deny   tcp any any eq 137
access-list 100 deny   tcp any any eq 138
access-list 100 deny   tcp any any eq 139
access-list 100 deny   tcp any any eq 445
access-list 100 deny   udp any any eq 135
access-list 100 deny   udp any any eq 136
access-list 100 deny   udp any any eq netbios-ns
access-list 100 deny   udp any any eq netbios-dgm
access-list 100 deny   udp any any eq 139
access-list 100 deny   udp any any eq 445
access-list 100 deny   tcp any any eq 4444
access-list 100 deny   udp any any eq tftp
access-list 100 permit ip any any
dialer-list 1 protocol ip permit
!
line con 0
line vty 0 4
 password remoteuser
 login
!
end

NBR#
```

4.2.3 DHCP 接入典型配置

如图 4-8，用户使用电缆通过 ISP(Internet Service Provide,Internet 服务提供商)接入 Internet。ISP(比如电信或者其他宽带服务提供商)使用 DHCP 为 WAN 口分配广域网地址，用户在 LAN 口上使用内部网地址 192.168.0.1，该地址即内部网关地址。用户在 LAN 和 WAN 口上配置了 NAT 以使内部网用户可以共享光纤线路来访问 Internet。

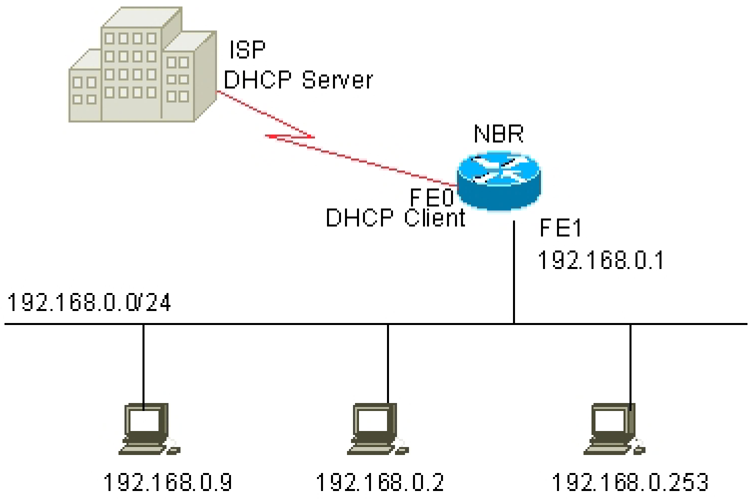


图 4-8 DHCP 接入典型配置

在这种情况下，就可以在 NBR 上如下配置即可：

!进入特权用户层
Red-Giant>enable
!启动快速配置功能
Red-Giant#setup
　　　　------------ 交互式系统配置 ----------------
输入 ctrl-c 中止配置流程；默认配置参数在'[]'中。
!选择是否进入快速配置流程
确定进入交互式系统配置? [yes]: **yes**
配置全局参数:
　请输入路由器名称（只能用字母数字组合） [Red-Giant]: NBR
!配置进入特权用户层的口令,这里 secret 与 password 同为进入用户层的口令，不过 secret 的安全性和优先级高于 password。
Enable secret 是一个单向的图形加密密钥,它优先于 enable password 被采用
　请输入 enable secret: **private**
Enable password 在没有配置 enable secret,
或者在使用旧的软件版本以及某些 boot 映象软件时被采用
　请输入 enable password: **puzzle**
!配置允许远程 Telnet 登陆的用户密码
　请输入虚拟终端登陆密码: **remoteuser**
!选择是否启动冲击波病毒防护功能。如果确认内部网没有感染冲击波病毒，建议不要启动该防护功能以免降低系统性能。
启动防止冲击波病毒功能会降低性能，如果没有病毒，可以不启动
是否启动此功能? [no]: **no**
!选择上网模式即 WAN 口接入 Internet 的模式,这里使用的是 DHCP 模式。
请选择上网模式:
　　　　1. 固定 IP 地址
　　　　2. PPPOE 连接
　　　　3. DHCP 分配 IP
请输入数字 1---3: **3**
!设置局域网口地址即本地网关地址
配置局域网口 FastEthernet1:
　请输入 IP 地址: **192.168.0.1**
　请输入地址掩码 [255.255.255.0]:
!由于内部网主机的 IP 地址是静态配置的，这里就无需启用 DHCP Server 功能

```
是否对内部局域网启用 DHCP SERVER 功能? [no]: no
！预览通过快速配置生产的配置脚本文件
配置完毕，生成的配置脚本文件如下:

hostname NBR
ip routing
enable secret 5 $1$4S/W$f498W8ZBcrVhvX7Bg/vOL.
enable password puzzle
line vty 0 4
password remoteuser
!
!
interface FastEthernet0
no shutdown
ip address dhcp
ip nat outside
!
!
interface FastEthernet1
no shutdown
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
ip nat inside source list 1 interface FastEthernet 0 overload
ip nat optimize
!
access-list 1 permit any
!
end
！选择保存并应用这份配置
是否应用此配置? [yes/no]: yes
Building configuration...
[OK]
%UPDOWN: Line protocol on Interface FastEthernet0, changed state to up
%UPDOWN: Line protocol on Interface FastEthernet1, changed state to up
%CHANGED: Interface Dialer0, changed state to administratively down
在 enabled 模式下使用'configure'命令可修改这些配置。
NBR#
%UPDOWN: Interface FastEthernet0, changed state to up
%UPDOWN: Interface FastEthernet1, changed state to up
！再次确认配置
NBR#show running-config
Building configuration...

Current configuration:
!
!
hostname "NBR"
!
enable secret 5 $1$4S/W$f498W8ZBcrVhvX7Bg/vOL.
enable password puzzle
!
!
!
ip subnet-zero
!
interface FastEthernet0
 ip address dhcp
 ip nat outside
```

```
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
!
ip nat inside source list 1 interface FastEthernet0 overload
ip nat optimize
ip classless
access-list 1 permit any
!
line con 0
line vty 0 4
 password remoteuser
 login
!
end

NBR#
```

4.2.4 构建私服典型配置(放到高级配置功能中)

这里的私服是指利用 NBR 将一个或者多个内部主机映射成网络服务器，从而使得广域网上的网络用户可以获得对应的服务。如图 4-9，用户在内部网内设置了三台服务器(FTP 服务器、WEB 服务器以及 E-MAIL 服务器)，他希望广域网上的网络主机能够访问这三个服务器。RGNOS 提供静态 NAT 映射功能来实现这些需求。

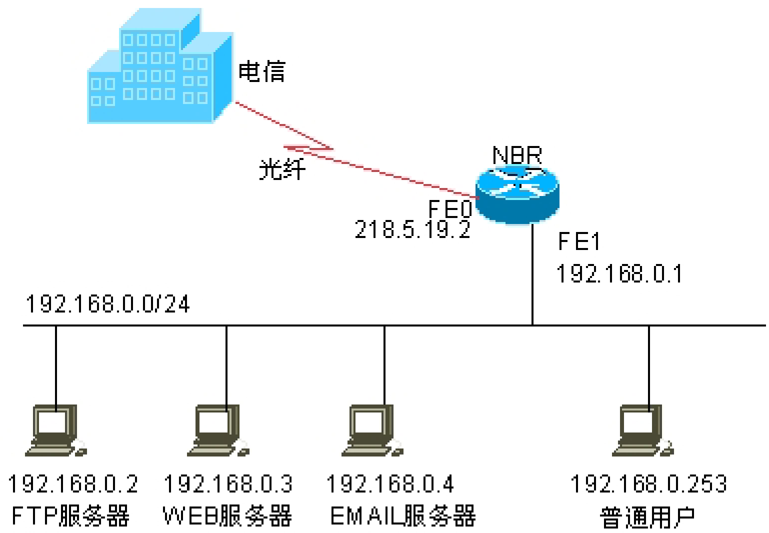


图 4-9 构建私服的典型配置示例

为了实现这些功能，需要配置 NAT 静态映射功能。快速配置功能中不包含该功能的设置，因此需要手动设置：

```
!进入特权用户层
Red-Giant>enable
!进入全局配置层
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!进入 WAN 口配置层
Red-Giant(config)#interface fastethernet 0
```

```
!配置 WAN 口地址
Red-Giant(config-if)#ip address 218.5.19.2 255.255.255.0
!设置 WAN 口为共享连接的 Internet 接入口
Red-Giant(config-if)#ip nat outside
!启用 WAN 口
Red-Giant(config-if)#no shut
!返回普通用户层
Red-Giant(config-if)#end
Red-Giant#
!这些是系统提示信息，系统提示 WAN 口链路处于 UP 状态(可通讯状态).
%UPDOWN: Line protocol on Interface FastEthernet0, changed state to up
%UPDOWN: Interface FastEthernet0, changed state to up
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!进入 LAN 口配置层
Red-Giant(config)#interface fastethernet 1
!配置 LAN 口地址
Red-Giant(config-if)#ip address 192.168.0.1 255.255.255.0
!设置 LAN 口为共享连接的 Intranet 接入口
Red-Giant(config-if)#ip nat inside
!启用 LAN 口
Red-Giant(config-if)#no shut
Red-Giant(config-if)#end
Red-Giant#
%UPDOWN: Line protocol on Interface FastEthernet1, changed state to up
%UPDOWN: Interface FastEthernet1, changed state to up
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!配置默认路由以访问 Internet
Red-Giant(config)#ip route 0.0.0.0 0.0.0.0 fastethernet 0 218.5.19.1
!配置 NAT 应用的访问列表
Red-Giant(config)#access-list 1 permit any
!配置连接共享规则
Red-Giant(config)#ip nat inside source list 1 interface fastethernet 0
!配置 FTP 服务器的静态映射
Red-Giant(config)#ip nat inside source static tcp 192.168.0.2 20 218.5.19.2
20
Red-Giant(config)#ip nat inside source static tcp 192.168.0.2 21 218.5.19.2
21
!配置 WEB 服务器的静态映射
Red-Giant(config)#ip nat inside source static tcp 192.168.0.3 80 218.5.19.2
80
!配置 EMAIL 服务器的静态映射
Red-Giant(config)#ip nat inside source static tcp 192.168.0.4 25 218.5.19.2
25
Red-Giant(config)#ip nat inside source static tcp 192.168.0.4 110 218.5.19.2
110
Red-Giant(config)#end
Red-Giant#
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!配置远程用户 Telnet 访问口令
Red-Giant(config)#line vty 0 4
Red-Giant(config-line)#password remoteuser
Red-Giant(config-line)#end
Red-Giant#
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Red-Giant(config)#enable password puzzle
!配置路由器名称
Red-Giant(config)#host NBR
NBR(config)#end
NBR#
!保存配置
NBR#write
Building configuration...
[OK]
NBR#
!检查配置
NBR#show running-config
Building configuration...

Current configuration:
!
!
hostname "NBR"
!
enable password puzzle
!
!
!
ip subnet-zero
!
interface FastEthernet0
 ip address 218.5.19.2 255.255.255.0
 ip nat outside
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
!
ip nat inside source list 1 interface FastEthernet0 overload
ip nat inside source static tcp 192.168.0.4 110 218.5.19.2 110
ip nat inside source static tcp 192.168.0.4 25 218.5.19.2 25
ip nat inside source static tcp 192.168.0.3 80 218.5.19.2 80
ip nat inside source static tcp 192.168.0.2 21 218.5.19.2 21
ip nat inside source static tcp 192.168.0.2 20 218.5.19.2 20
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0 218.5.19.1
access-list 1 permit any
!
line con 0
line vty 0 4
 password remoteuser
 login
!
end

NBR#
```

第五章 高级配置指导

5.1 配置 IP 地址

IP 地址配置任务包括以下各项，但只有第一项配置是必须要做，其它任务可以根据网络的具体需要决定是否要执行。

- 接口 IP 地址配置(必须)
- 地址解析协议(ARP)配置(可选)
- 主机名到 IP 地址映射配置(可选)
- 关闭 IP 路由(可选)
- 广播包处理配置(可选)

5.1.1 接口 IP 地址配置

一个设备只有配置了 IP 地址，才可以接收和发送 IP 数据报，接口配置了 IP 地址，说明该接口允许运行 IP 协议。要分配一个接口的 IP 地址，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)#**ip address** *ip-address mask*	设置一个接口的 IP 地址
Red-Giant(config-if)#**no ip address**	取消一个接口的 IP 地址配置

网络掩码也是一个 32 位比特的数值，标识着该 IP 地址的哪几个比特为网络部分。

RGNOS 软件可以支持一个接口配置多个 IP 地址，其中一个为主 IP 地址，其余全部为次 IP 地址。次 IP 地址的配置理论上没有数目限制，可以随意配置。要配置次 IP 地址，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)#**ip address** *ip-address mask* **secondary**	设置接口次 IP 地址
Red-Giant(config-if)#**no ip address** *ip-address mask* **secondary**	取消接口次 IP 地址配置

RGNOS 支持无编号(*unnumbered*)接口功能。无编号接口就是只在接口启动 IP 协议，但是不分配 IP 地址，无编号接口需要关联一个具有 IP 地址的接口。无编号接口产生的 IP 数据包，该数据包的源 IP 地址为关联接口的 IP 地址。另外路由协议进程也根据关联接口的 IP 地址，决定是否往无编号接口发送路由更新报文。要配置无编号接口，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)# **ip unnumbered** *接口类型 接口编号*	配置无编号接口的关联接口

Red-Giant(config-if)# **no ip unnumbered**	取消无编号接口配置

5.1.2 地址解析协议(ARP)配置

通常情况下，不需要特别配置，路由器已经启动地址解析功能。RGNOS 允许用户通过配置来控制地址解析功能。

ARP 协议提供了 IP 地址和 MAC 地址动态映射的功能。RGNOS 允许用户通过配置静态 ARP，还可以响应不是属于自己 IP 地址的 ARP 请求。要配置静态 ARP，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**arp** *ip-address mac-address arp-type*	定义静态 ARP
Red-Giant(config)#**arp** *p-address mac-address arp-type* **alias**	响应该 IP 地址的 ARP 请求
Red-Giant(config)#**no arp** *ip-address*	取消静态 ARP

缺省情况下，ARP 封装为 Ethernet II 类型，在 RGNOS 中表示为 *arpa* 关键字。根据网络的需要，你还可以封装为 SNAP 类型。不管 ARP 封装哪种类型，RGNOS 都可以响应两种类型封装的 ARP 请求。如果 ARP 封装为 SNAP 类型，RGNOS 可以发送两种类型的 ARP 请求 如果 ARP 封装为 ARPA 类型,RGNOS 只发送 ARPA 类型的 ARP 请求。要配置 ARP 封装，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)#**arp** {**arpa** | **snap**}	设置 ARP 封装类型
Red-Giant(config-if)#**no arp** {**arpa** | **snap**}	取消 ARP 封装类型设置

如果明确取消 ARPA 封装，该接口将不会发送和响应 ARPA 封装的 ARP 请求。

ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射有效。超时时间设置得越短，ARP 缓冲中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多，所以需要权衡利弊。要配置 ARP 超时时间，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)#**arp timeout** *seconds*	配置 ARP 超时时间
Red-Giant(config-if)#**no arp timeout**	恢复缺省配置

缺省情况下，超时时间为 14400 秒，即 4 个小时。

路由器的代理 ARP 功能可以帮助没有路由信息的主机，获得与其它网络或子网通讯的能力。比如路由器接收到一个 ARP 请求，ARP 请求发送者的 IP 地址与所请求的 IP 地址不属于同一网络，而路由器又知道所请求 IP 地址的路由，路由器就会发送 ARP 响应，响应的 MAC 地址为路由器自身的以太网 MAC 地址，以上过程就是代理 ARP 的功能。要配置代理 ARP，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)# **ip proxy-arp**	启用代理 ARP 功能

Red-Giant(config-if)# **no ip proxy-arp**	关闭代理 ARP 功能

5.1.3 主机名到 IP 地址映射配置

主机名到 IP 地址的映射有两种方式：1).静态映射，每台设备上都配置主机到 IP 地址的映射，各设备独立维护自己的映射表，而且只供本设备使用；2).动态映射，通过域名解析系统(DNS)实现。通过主机名，最终得到该主机名对应的 IP 地址的过程叫做域名解析(主机名解析)。RGNOS 支持在本地进行主机名解析，也支持通过 DNS 进行域名解析。配置主机名到 IP 地址的映射，RGNOS 提供三种途径：1).静态配置主机名和 IP 地址映射；2).动态学习主机名和 IP 地址映射；3).定义缺省域名。

在全局配置模式中执行以下命令可以实现静态配置主机名和 IP 地址映射：

命令	作用
Red-Giant(config)#**ip host** *host-name* [*Telnet-port*] *ip-address* [*ip-address2*…*ip-address8*]	手工配置主机名和 IP 地址映射
Red-Giant(config)#**no ip host**	删除手工配置

telnet-port 缺省值为 TCP 23 号端口。配置参数 *telnet-port*，主要是用于反向 Telnet。反向 Telent 可以对路由器异步线路直连的设备（可以是 Modem，或者其它路由器）进行互操作。telnet-port 的取值为“ 2000 + 异步线路编号 ”，该编号可以用 show line 看到。

动态学习是指通过 DNS 服务器学习主机名和 IP 地址映射，并将结果保存在本地的映射表中。在全局配置模式中执行以下命令可以实现动态学习主机名和 IP 地址映射：

命令	作用
Red-Giant(config)#**ip name-server** *ip-address* [*ip-address2*…*ip-address 6*]	配置 DNS 服务器，最多可以有 6 个
Red-Giant(config)#**ip domain-lookup**	启动 DNS 进行域名解析
Red-Giant(config)#**no ip name –server**	删除 DNS 服务器
Red-Giant(config)#**no ip domain-lookup**	关闭 DNS 域名解析

缺省情况下是进行域名解析，即使没有配置 DNS 服务器，如果你在执行命令模式中随便输入一串字符，也会尝试进行域名解析，不过请求包是广播报文。如果你不希望出现这种情况，可以关闭 DNS 域名解析。

如果定义了缺省域名，当路由器进行域名解析时，对于不完整的主机名会自动加上缺省域名做后缀形成一个完整的主机名，然后进行解析。比如缺省域名定义为“ *com.cn* ”,在路由器上执行“ ***ping*** *myhost* ”,路由器会自动在主机名“ *myhost* ”加上缺省的域名“ *com.cn* ”，然后查找主机名“ *myhost.com.cn* ”对应的 IP 地址。要配置缺省域名，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip domain-name** *domain-name*	定义缺省域名

Red-Giant(config)#**ip domain-list** *domain-name*	增加域名到域名列表中
Red-Giant(config)#**no ip domain-name** *domain-name*	取消缺省域名
Red-Giant(config)#**no ip domain-list** *domain-name*	删除域名列表中的某个域名

你可以通过域名列表定义多个域名。对于不完整的主机名，路由器将按顺序查找域名列表中定义的后缀域名，DNS 会请求解析完整主机名的 IP 地址，如果所有的后缀域名与不完整主机名的组合都不能解析到 IP 地址，RGNOS 软件就会提示不存在该主机。配置了后缀域名列表，通过命令 **ip domain-name** 定义的缺省域名将失效。

说明：

配置 *ip domain-list* 命令，使用 Connect 和 Telnet 命令跟主机名时，如果主机名的后缀域名不在域名列表中，必须写全主机域名并以点做结尾。

5.1.4 关闭 IP 路由

IP 路由功能缺省情况下是启动的，除非你确定不需要 IP 路由功能，否则不要执行该操作。关闭 IP 路由将使路由器丢失所有的路由，而且没有路由转发的功能。

要关闭 IP 路由功能，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**no ip routing**	关闭 IP 路由功能
Red-Giant(config)#**ip routing**	启动 IP 路由功能

关闭了 IP 路由功能的路由器，在网络功能上相当于 PC 机。但是该路由器还可以与其它网络设备通讯，与外界通讯主要借助于：1).代理 ARP；2).缺省网关。关闭了 IP 路由后，缺省网关特性将自动变为有效。代理 ARP 的配置在上文已有描述，这里不再赘述。

在全局配置模式中执行以下命令可以配置缺省网关：

命令	作用
Red-Giant(config)#**ip default-gateway** *ip-address*	配置缺省网关
Red-Giant(config)#**no ip default-gateway**	取消缺省网关

只有当关闭 IP 路由后，缺省网关才有效。如果启动了 IP 路由，缺省网关将失效。

5.1.5 广播包处理配置

如果 IP 网络设备转发淹没广播，可能会引起网络的超负载，严重影响网络的运行，这种情况称为广播风暴。路由器提供了一些办法能够将广播风暴限制在本地网络，阻止其继续扩张。但对于桥和交换机等基于二层网络设备，将转发和传播广播风暴。解决广播风暴最好的办法就是给每个网络指定一个广播地址，这就是定向广播，这要求使用广播包的 IP 协议尽可能应用定向广播而不是淹没广播进行数据传

播。RGNOS 提供三种途径来控制广播：1).定向网络广播到物理广播转换；2).UDP 广播包和协议转发；3).创建 IP 广播地址。

IP 定向广播报文是指目标地址为某个 IP 子网广播地址的 IP 报文，如目标地址为 172.16.16.255 的报文就称为定向广播报文。但是产生该报文的节点又不是目标子网的成员。没有与目标子网直连的路由器接收到 IP 定向广播报文，跟转发单播报文一样处理定向广播报文。你可以在指定的接口上，启动定向广播到物理广播转换的功能，这样该接口就可以转发到直连网络的定向广播了。该命令只影响已到最终目标子网的定向广播报文的最后传输。在接口配置模式中执行以下命令来配置定向广播到物理广播的转换：

命令	作用
Red-Giant(config-if)#**ip directed-broadcast** [*access-list-number*]	在接口上，启动定向广播到物理广播的转换
Red-Giant(config-if)#**no ip directed-broadcast**	取消转换

网络上的主机有时需要使用 UDP 广播包来获取 IP 地址、配置信息、名字信息。如果主机所在的网络没有这样的服务器，UDP 广播通常又不转发，该主机就不能正常工作了。你可以通过配置与主机在同一网络的路由器接口，当该接口接收到该类广播包时，将转发到指定的 IP 地址(称为 Helper 地址)上。一个接口配置了 Helper 地址后，如果你没有配置需要转发哪些 UDP 广播包，缺省情况下，该路由器将作为 BOOTP 转发代理。配置 UDP 广播并指定目标地址，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)#**ip helper-address** *ip-address*	配置将 UDP 广播包转发到指定的 IP 地址，如 DHCP 包。
Red-Giant(config-if)#**no ip helper-address** *ip-address*	取消将 UDP 广播包转发到指定的 IP 地址

如果需要转发其它的 UDP 广播包，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	通过 UDP 端口定义转发哪些协议

说明：

RGNOS 软件版本在启用 DHCP 中继代理时，需要关闭 DHCP 服务器。将来版本可以同时支持 DHCP 中继代理和 DHCP 服务器。

当前使用最多的广播包，其目标地址为全“1”，表示为 255.255.255.255。RGNOS 可以通过软件定义产生其它地址的广播包，而且可以接收所有类型的广播包。要配置有别于 255.255.255.255 的广播地址，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)#**ip broadcast-address** *ip-address*	创建新的广播地址
Red-Giant(config-if)#**no ip broadcast-address**	取消新的广播地址

5.1.6 IP 地址配置示例

下面给出一个 IP 地址配置示例：

```
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Red-Giant(config)#interface fastethernet 0
Red-Giant(config-if)#ip add 192.168.20.3 255.255.255.0
Red-Giant(config)#end
Red-Giant#
```

5.2 配置静态路由

5.2.1 配置静态路由

静态路由就是手工配置的路由，使得到指定目标网络的数据包的传送，按照预定的路径进行。要配置静态路由，需在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip route** *network mask* {ip-address | *interface-type interface-number* } [*distance*] [**tag** *tag*] [**permanent**]	配置静态路由
Router(config)#**no ip route** *network mask*	删除静态路由

如果没有执行删除动作，RGNOS 将永久保留静态路由。当一个接口处于“ down ”状态时，所有指向该接口的路由将全部从路由表中消失。另外，当 RGNOS 找不到静态路由下一跳地址的转发路由时，该静态路由也会从路由表中消失。

5.2.2 静态路由配置示例

下面给出一个静态路由配置示例：

```
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Red-Giant(config)#ip route 0.0.0.0 0.0.0.0 fastethernet 0 192.168.12.1
Red-Giant(config)#end
Red-Giant#
```

5.3 配置防火墙

访问控制列表(access control lists)，也称为访问列表(access lists)，俗称为防火墙，是通过定义一些准则对经过路由器接口上的数据报文进行控制：转发或丢弃。访问列表准则可以针对数据流的源地址、目标地址、上层协议或其他信息。RGNOS

允许用户使用以下几类访问列表：1).基本访问列表；2).动态访问列表；3).基于时间的访问列表。

5.3.1 配置基本访问列表

基本访问列表的配置包括以下两步：1).定义基本访问列表；2).将基本访问列表应用于特定接口。要配置基本访问列表，请在全局配置模式下执行以下命令：

命令	作用
Red-Giant(config)# **access-list** *access-list-number* {**permit|deny**} […...]	定义访问列表(必须)
Red-Giant(config)# **interface** *type number*	选择要应用访问列表的接口(必须)
Red-Giant(config-if)# **ip access-group** *access-list-number* {**in|out**}	将访问列表应用特定接口(必须)

5.3.2 配置动态访问列表

动态访问列表也称为锁定和密钥(*Lock-and-Key*)，可以动态地过滤 IP 报文分组。在配置了动态访问列表后，路由器上动态访问列表的运行过程如下：1).首先用户打开一个到边界路由器(防火墙)的 *Telnet* 会话；2).RGNOS 打开 *TELNET* 会话，提示用户输入用户名和密码，并对用户进行身份认证；3).通过身份认证用户后，RGNOS 断开 *TELNET* 会话，此时生成一个临时选项，路由器使用该选项对用户的数据进行管理；4).用户通过防火墙即边界路由器进行交换数据；5).当配置的定时器时间到期的时候，RGNOS 删除临时选项。系统管理员也可以在手工删除临时选项。要配置动态访问列表，需要安装下面的顺序进行相应的配置：

命令	作用
Red-Giant(config)#**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] { **deny** |**permit**} ...	定义访问列表(必须)
Red-Giant(config)#**access-list dynamic-extend**	扩展记录存活时间(可选)
Red-Giant(config)#**interface** *type number*	选择要应用访问列表的接口(必须)
Red-Giant(config-if)# **ip access-group** *access-list-number* {**in|out**}	将访问列表应用特定接口(必须)
Red-Giant (config-if)#**exit**	退出当前配置层
Red-Giant(config)# **line vty** *line-number* *[ending-line-number]*	选择 Telnet 接入对应的 VTY 接口(必须)

Red-Giant(config-line)# **login** [**local**] or Red-Giant(config)# **username** *name* **password** *secret* or Red-Giant(config-line)# **password** *password*	配置用户身份验证信息(必须)
Red-Giant(config-line)# **autocommand access-enable** *host* [**timeout** *minutes*]	配置动态访问列表触发命令(必须)

5.3.3 配置基于时间的访问列表

RGNOS 提供基于时间的 ACL 功能。使用该功能，网络管理员就可以依据时间来控制用户对网络资源的访问，例如可以根据时间来禁止/允许用户访问网络资源或者改变访问网络的路由。为了使用基于时间的 ACL 功能，必须首先创建一个对应的 Time-range 接口来指明时间与日期。然后，就将 Time-range 接口与对应的 ACL 关联起来。为了配置基于时间的 ACL 功能，需要完成下面的配置任务：1).校正路由器实时时钟(必须)；2).创建并定义 Time-range 接口(必须)；3).关联 ACL 与 Time-range 接口(必须)；4).在网络接口上应用基于时间的 ACL(必须)。

校正路由器实时时钟。该项功能的典型设置如下:

命令	目的
Red-Giant# **enable**	进入特权用户层
Red-Giant# **clock set** *hh: mm: ss date month year* or Red-Giant# **clock set** *hh: mm: ss month date year*	设置系统时钟(时间以及日期)
Red-Giant# **clock update-calendar**	依据当前设置更新实时时钟(硬件)
Red-Giant# **disable**	退出特权用户层

创建并定义 Time-range 接口。该项功能的典型设置如下：

命令	目的
Red-Giant# **config terminal**	进入全局配置层
Red-Giant(config)# **time-range** *time-range-name*	进入/创建指定名称的 time-range 接口
Red-Giant(config-time-range)# **absolute** *[***start** *time date] [***end** *time date]* and/or **periodic** *days-of-the-week hh:mm* **to** [*days-of-the- week*] *hh:mm*	进入 time-range 配置层，设置限制的时间段。其中,只允许配置一个 absolute 规则,但允许多个 periodic 规则并存
Red-Giant(config-time-range)#**exit**	退出 time-range 配置层

关联 ACL 与 Time-range 接口。RGNOS 只允许扩展的 ACL 关联 Time- range 接口。该项功能的典型设置如下：

命令	目的
Red-Giant# **config terminal**	进入全局配置层
Red-Giant(config)# **access-list** *number* [**dynamic** *dyn-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source src-wildcard destination desti-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range- name*] and/or **access-list** number [**dynamic** *dyn-name* [**timeout** *minutes*]] {**deny** | **permit**} **icmp** *source src-wildcard destination desti-wildcard* [**icmptype** | [[**icmptype** *icmpcode*] | [*icmpmessagecode*]] [**prece dence** *precedence*] [**tos** tos] [**log**] [**timerange** *time-range-name*] and/or **access-list** *number* [**dynamic** *dyn-name* [**timeout** *minutes*]] {**deny** | **permit**} **tcp** *source src-wildcard* [*operator* [*port*]] *destination desti-wildcard* [*operator* [*port*]] [**established**] [**precedence** *preced ence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] and/or **access-list** *number* [**dynamic** *dyn-name* [**timeout** *minutes*]] {**deny** | **permit**} **udp** *source src-wildcard* [*operator* [*port*]] *destination desti-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] and/or **access-list** *number* [**dynamic** *dyn-name* [**timeout** *minutes*]] {**deny** | **permit**} **igmp** *source src-wildcard destination desti-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*]	设置扩展的 ACL，并将 Time-range 关联到 ACL 上
Red-Giant(config)#**exit**	退出全局配置层

在网络接口上应用基于时间的 ACL。用户可以在指定的网络接口上应用基于时间的 ACL，就像应用其它类型的 ACL 一样，这里不再赘述。

5.3.4 防火墙配置示例

下面是一个基本访问列表配置示例：

```
interface FastEthernet0
 ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet1
 ip address 2.2.2.2 255.255.255.0
 ip access-group 101 in
 ip access-group 101 out
!
```

```
ip route 0.0.0.0 0.0.0.0 FastEthernet1 2.2.2.1
!
access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet
access-list 101 deny  icmp 192.168.12.0 0.0.0.255 any
access-list 101 deny  ip 2.2.2.0 0.0.0.255 any
```

下面是一个动态访问列表配置示例：

```
interface FastEthernet0
ip address 172.18.23.9 255.255.255.0
ip access-group 101 in

access-list 101 permit tcp any host 172.18.21.2 eq telnet
access-list 101 dynamic mytestlist timeout 120 permit ip any any

line vty 0 4
login local
autocommand access-enable timeout 5
```

下面是一个基于时间的 ACL 的配置示例：

```
interface FastEthernet 0
 ip access-group 101 in
!
access-list 101 permit ip any any time-range xyz
!
time-range xyz
 absolute start 12:00 1 January 2001
```

5.4 配置 PPPoE

RGNOS 支持在以太网口上运行 PPP(PPPOE，PPP over Ethernet)，进行按需拨号，有数据通信则刺激拨号，空闲指定时间以后，自动挂断线路。PPPOE 配置包括以下三个方面：

- 配置以太网口
- 配置逻辑接口
- 配置全局参数

5.4.1 配置以太网口

以太网口配置任务包括以下部分：1).使能接口 PPPOE；2).绑定以太网口到指定的拨号池。当然，以太网口的其它一些基本配置是必须的，如接口激活(no shutdown)等。要使能以太网口的 PPPOE，请在接口配置模式下执行以下命令：

命令	作用
Red-Giant(config-if)#**pppoe enable**	启用 PPPOE

由于 RGNOS 的 PPPOE 是按需拨号的，故必须将以太网接口绑定到指定的拨号池，供逻辑接口进行按需拨号使用。要绑定以太网口到指定的拨号池，请在接口配置模式下执行以下命令：

命令	作用
Red-Giant(config-if)#**pppoe-client dial-pool-number** *pool-number* **dial-on-demand**	将以太网口绑定到逻辑接口指定的逻辑拨号池

dial-on-demand	

注意：

dail-on-demand 必须配置，该选项启用 PPPOE 按需拨号功能，如果没有配置该选项会导致无法使用自动拨号、空闲指定时间挂断线路等按需拨号功能。

5.4.2 配置逻辑接口

配置逻辑接口。PPPoE 拨号所有的 PPP 协商均建立在逻辑接口上的，故须在逻辑接口上配置相关参数。要配置逻辑接口，请在全局配置模式下执行以下命令：

命令	作用
Red-Giant(config)#**interface diale**r *dialer-number*	进入指定的接口
Red-Giant(config-if)#**ip address negotiate**	地址由协商获得
Red-Giant(config-if)#**dialer pool** *pool-number*	关联拨号池
Red-Giant(config-if)#**dialer idle-timeout** *seconds*	(可选)配置最大空闲时间
Red-Giant(config-if)#**encapsulation ppp**	封装 PPP
Red-Giant(config-if)#**mtu** *mtu-number*	设置最大传输单元
Red-Giant(config-if)#**dialer-group** *dialer-group-number*	与 dialer-list 对应，关联刺激拨号的规则。
Red-Giant(config-if)#**ppp pap sent-username** *username* **password** *password*	配置认证使用的用户名和密码。

说明：

以上配置命令除了第四步命令为可选命令以外，其他命令均必须配。特别是第六步 MTU 的值至少设置为 1492(建议设置为 1488，不能大于 1492)，否则无法正常通信。

另外建议联系 ISP 以确认合适的 MTU，有的 ISP(如某些地方的典型局端)要求将 MTU 必须设置为 1488，而有的 ISP 要求将 MTU 必须设置为 1492。

5.4.3 配置必要的全局参数

配置必要的全局参数。PPPoE 必要的全局参数，主要包括如下：1).定义拨号刺激规则；2).配置拨号路由。如果配合其他功能(如 NAt)一起使用 PPPoE，则还需要进行其它的配置，请根据具体的情况进行配置。要定义 PPPoE 拨号刺激规则，请在全局配置模式下执行以下命令：

命令	作用
Red-Giant(config)#**dialer-list** *number dialer-group* **protocol** *protocol-name*	定义刺激拨号的规则

{**permit** | **deny** | **list** *access-list-number* | *access-group*}	

由于接口的 IP 地址一般情况下是协商获得，没有逻辑接口的直连路由，所以为了使数据通过 PPPoE 的接口进行转发，还必须配置一条目标接口为进行 PPPoE 拨号的逻辑接口的拨号路由。要配置拨号路由，请在全局配置模式下执行以下命令：

命令	作用
Red-Giant(config)#**ip route 0.0.0.0 0.0.0.0 dialer** *dialer-number* [**permanent**]	配置默认路由。

说明：

当然拨号路由可以不用配置成默认路由，可以根据需要配置指定的路由。但无论什么情况，都要配置一条拨号路由，否则就无法拨号。

5.4.4 PPPoE 配置示例

```
hostname "Red-Giant"
!
ip subnet-zero
!
interface FastEthernet0
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 10 dial-on-demand
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip mtu 1492
 ip nat inside
!
interface Dialer1
 ip address negotiate
 mtu 1492
 encapsulation ppp
 ip nat outside
 dialer pool 10
 dialer-group 1
 dialer idle-timeout 300
 ppp pap sent-username pppoe password 0 pppoe
!
ip nat inside source list 1 interface Dialer1 overload
ip classless
 access-list 1 permit any
ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
!
dialer-list 1 protocol ip permit
!
line con 0
line aux 0
line vty 0 4
 login
!
```

end

5.5 配置 DHCP

DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)为互联网上主机提供配置参数。DHCP 是基于 Client/Server 工作模式，DHCP 服务器为需要动态配置的主机分配 IP 地址和提供主机配置参数。DHCP 有三种机制分配 IP 地址：1).自动分配，DHCP 给客户端分配永久性的 IP 地址；2).动态分配，DHCP 给客户端分配过一段时间会过期的 IP 地址(或者客户端可以主动释放该地址)；3).手工配置，由网络管理员给客户端指定 IP 地址。三种地址分配方式中，只有动态分配可以重复使用客户端不再需要的地址。配置 DHCP 包括下列配置任务：

- 启用 DHCP 服务器与中继代理(必须)
- DHCP 排斥地址配置(可选)
- DHCP 地址池配置(必须)
- 手工地址绑定(可选)
- 配置客户端启动文件(可选)
- 配置 Ping 包次数(可选)
- 配置 Ping 包超时时间(可选)
- 以太网接口 DHCP 客户端配置(可选)

5.5.1 启用 DHCP 服务器与中继代理

缺省情况下，RGNOS 启用了 DHCP 服务器同时关闭了 DHCP 中继代理，这两者不能并存。全局配置模式中执行以下命令来控制启用何种功能：

命令	作用
Red-Giant(config)#**service dhcp**	启用 DHCP 服务器,关闭 DHCP 中继代理
Red-Giant(config)#**no service dhcp**	启用 DHCP 中继代理,关闭 DHCP 服务器

说明：

RGNOS 软件在启用 DHCP 中继代理时，需要关闭 DHCP 服务器。

5.5.2 DHCP 排斥地址配置

要控制哪些地址不能分配给客户端，可以在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip dhcp excluded-address** *start-address end-address*	定义 IP 地址范围,这些地址 DHCP 不会分配给客户端
Red-Giant(config)#**no ip dhcp excluded-address**	取消配置地址排斥

start-address end-address	

5.5.3 DHCP 地址池配置

DHCP 的地址分配以及给客户端传送的 DHCP 各项参数，都需要在 DHCP 地址池中进行定义。要配置 DHCP 地址池，需要完成以下配置任务：

命令	作用
Red-Giant(config)#**ip dhcp pool** *dhcp-pool-name*	配置地址池名并进入地址池配置模式(必须)
Red-Giant(config-dhcp)#**network** *sub-network* [*mask*]	配置 DHCP 地址池的用于分配的网络地址的范围(必须)
Red-Giant(config-dhcp)#**default-router** *address* [*address1…address8*]	配置 DHCP 客户端的缺省网关(必须)
Red-Giant(config-dhcp)#**lease** {*days* [*hours*] [*minutes*] | **infinite**}	配置分配给 DHCP 客户端的网络地址租期(可选)
Red-Giant(config-dhcp)#**domain-name** *domain*	配置 DHCP 客户端的域名(可选)
Red-Giant(config-dhcp)#**netbios-name-server** *address* [*address1…address8*]	配置 DHCP 客户端的 NetBios WINS 服务器(可选)
Red-Giant(config-dhcp)#**dns-server** *address* [*address1…address8*]	配置 DHCP 客户端的 DNS 服务器(可选)
Red-Giant(config-dhcp)#**netbios-node-type** *type*	配置 DHCP 客户端的 NetBios 节点类型(可选)

5.5.4 手工地址绑定

地址绑定是指 IP 地址和客户端 MAC 地址的映射关系。要定义手工地址绑定，首先需要定义主机地址池，然后定义 DHCP 客户端的 IP 地址和硬件地址或客户端标识。硬件地址就是 MAC 地址。微软客户端一般定义客户端标识，而不定义 MAC 地址，客户端标识包含了网络媒介类型和 MAC 地址。要配置手工地址绑定，在地址池配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip dhcp pool** *name*	定义地址池名，进入 DHCP 配置模式(必须)
Red-Giant(config-dhcp)#**host** *address*	定义客户端 IP 地址(必须)
Red-Giant(config-dhcp)#**hardware-address** *hardware-address type* *or* Red-Giant(config-dhcp)#**client-identifier** *unique-identifier*	定义客户端硬件地址(必须) 定义客户端的标识(必须)

Red-Giant(config-dhcp)#**client-name** *name*	(可选)标识客户端名称

5.5.5 配置客户端启动文件

客户端启动文件是客户端启动时要用到的启动映像文件。启动映像文件通常是 DHCP 客户端需要下载的操作系统。

要配置客户端的启动文件，在地址池配置模式中执行以下命令：

命令	作用
Router(dhcp-config)#**bootfile** *filename*	配置客户端启动文件名

5.5.6 配置 Ping 包次数

缺省情况，当 DHCP 服务器试图从地址池中分配一个 IP 地址时，会对该地址执行两次 Ping 命令(一次一个数据包)。如果 Ping 没有应答，DHCP 服务器认为该地址为空闲地址，就将该地址分配给 DHCP 客户端；如果 Ping 有应答，DHCP 服务器认为该地址已经在使用，就试图分配另外一个地址给 DHCP 客户端。要配置 Ping 包次数，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip dhcp ping packets** *number*	配置 Ping 包次数

5.5.7 配置 Ping 包超时时间

缺省情况下，DHCP 服务器 Ping 操作如果 500 毫秒没有应答，就认为没有该 IP 地址主机存在。你可以通过调整 Ping 包超时时间，改变服务器 Ping 等待应答的时间。要配置 Ping 包超时时间，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip dhcp ping timeout** *milliseconds*	配置 Ping 包超时时间。

5.5.8 以太网接口 DHCP 客户端配置

RGNOS 支持以太网端口通过 DHCP 获得动态分配的 IP 地址。要配置以太网接口 DHCP 客户端，在接口配置模式中执行以下命令：

命令	作用
Red-Giant(config-if)#**ip address dhcp**	配置通过 DHCP 得到 IP 地址

5.5.9 DHCP Server 配置示例

在以下配置中，定义了一个地址池 net172，地址池网段为 172.16.1.0/24，缺省网关为 172.16.16.254，域名为“ *rg.com* ”，域名服务器为 172.16.1.253，WINS 服务器为 172.16.1.252，NetBIOS 节点类型为复合型，地址租期为 30 天。该地址池中除了 172.16.1.2~172.16.1.100 地址外，其余地址均为可分配地址。

```
ip dhcp excluded-address 172.16.1.2 172.16.1.100
!
ip dhcp pool net172
network 172.16.1.0 255.255.255.0
default-router 172.16.1.254
domain-name rg.com
dns-server 172.16.1.253
netbios-name-server 172.16.1.252
netbios-node-type h-node
lease 30
```

5.5.10 DHCP Client 配置示例

以下配置中，路由器接口 FastEthernet0 配置了 DHCP 自动分配地址。

```
interface FastEthernet0
ip address dhcp
```

5.6 配置 NAT

在配置 NAT(网络地址转换)之前，你首先需要了解内部本地地址和内部全局地址的分配情况。根据你对 NAT 不同的需要，可以执行以下不同的任务来达到目的。

- 内部源地址 NAT 配置
- 内部源地址 NAPT 配置
- 重叠地址 NAT 配置
- TCP 负载均衡
- 调整 NAT 超时时间

5.6.1 配置内部源地址 NAT

当内部网络需要与外部网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。你可以配置静态或动态的 NAT 来实现互联互通的目的，或者需要同时配置静态和动态的 NAT。

静态 NAT，是建立内部本地地址和内部全局地址的一对一永久映射。当外部网络需要通过固定的全局可路由地址访问内部主机，静态 NAT 就显得十分重要。要配置静态 NAT，在全局配置模式中执行以下命令：

命令	作用

Red-Giant(config)#**ip nat inside source static** *local-address global-address*	定义内部源地址静态转换关系
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat inside**	定义该接口连接内部网络
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat outside**	定义该接口连接外部网络

以上配置为最简单配置，你可以配置多个 **Inside** 和 **Outside** 接口。

动态 NAT，是建立内部本地地址和内部全局地址池的临时映射关系，过一段时间没有用就会删除映射关系。要配置动态 NAT，在在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*}	定义全局 IP 地址池
Red-Giant(config)#**access-list** *access-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换
Red-Giant(config)#**ip nat inside source list** *access-list-number* **pool** *address-pool*	定义内部源地址动态转换关系
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat inside**	定义接口连接内部网络
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat outside**	定义接口连接外部网络

说明：

访问列表的定义，使得只在列表中许可的源地址才可以被转换，必须注意访问列表最后一个规则是否定全部。访问列表不能定义太宽，要尽量准确，否则将出现不可预知的结果。

5.6.2 配置内部源地址 NAPT

传统的 NAT 一般是指一对一的地址映射，不能同时满足所有的内部网络主机与外部网络通讯的需要。使用 NAPT，可以将多个内部本地地址映射到一个内部全局地址。

要配置静态 NAPT，在全局配置模式中执行以下命令：

命令	作用

Red-Giant(config)#**ip nat inside source static** {**UDP** | **TCP**}　*local-address port global-address port*	定义内部源地址静态转换关系
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat inside**	定义该接口连接内部网络
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat outside**	定义接口连接外部网络

要配置内部源地址动态 NAPT，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip nat pool**　*address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*}	定义全局 IP 地址池，对于 NAPT，一般就定义一个 IP 地址
Red-Giant(config)#**access-list** *access-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换
Red-Giant(config)#**ip nat inside source list** *access-list-number* {[**pool** *address-pool*] | [**interface** *interface-type interface-number*]}　**overload**	定义源地址动态转换关系
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat inside**	定义接口连接内部网络
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat outside**	定义接口连接外部网络

NAPT 可以使用地址池中的 IP 地址，也可以直接使用接口的 IP 地址。一般来说一个地址就可以满足一个网络的地址转换需要，一个地址最多可以提供 64512 个 NAT 地址转换。如果地址不够，地址池可以将多定义几个地址。

5.6.3 配置重叠地址 NAT

两个需要互联的私有网络分配了同样 IP 地址，或者一个私有网络和公有网络分配了同样的全局 IP 地址，这种情况称为地址重叠。两个重叠地址的网络主机之间是不可能通信的，因为它们相互认为对方的主机在本地网络。重叠地址 NAT 就是专门针对重叠地址网络之间通信的问题，配置了重叠地址 NAT，外部网络主机地址在内部网络表现为另一个网络主机地址，反之一样。

重叠地址 NAT 配置，其实分为两个部分内容：1).内部源地址转换配置，如何配置请参见上文；2)外部源地址转换配置，只有与内部网络地址重叠的外部网络需要配置外部源地址转换，外部源地址转换可以采用静态 NAT 配置或动态 NAT 配置。

要配置外部源地址的静态 NAT，在全局配置模式中执行以下命令：

命令	作用

Red-Giant(config)#**ip nat outside source static** *global-address local-address*	定义外部源地址静态转换关系
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat inside**	定义该接口连接内部网络
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat outside**	定义接口连接外部网络

要配置外部源地址的动态 NAT，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*}	定义本地 IP 地址池
Red-Giant(config)#**access-list** *access-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换
Red-Giant(config)#**ip nat outside source list** *access-list-number* **pool** *address-pool*	定义外部源地址动态转换关系
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat inside**	定义接口连接内部网络
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat outside**	定义接口连接外部网络

5.6.4 配置 TCP 负载均衡

当内部网络某台主机 TCP 流量负载过重时，可用多台主机进行 TCP 业务的均衡负载。这时，可以考虑用 NAT 来实现 TCP 流量的负载均衡。NAT 创建了一台虚拟主机提供 TCP 服务，该虚拟主机对应内部多台实际的主机，然后对目标地址进行轮询置换，达到负载分流的目的。要配置目标地址轮询转换，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*}	定义 IP 地址池，包含所有实际主机地址
Red-Giant(config)#**access-list** *access-list-number* **permit** *ip-address wildcard*	定义访问列表，只匹配虚拟主机地址
Red-Giant(config)#**ip nat inside destination list** *access-list-number* **pool** *address-pool*	定义内部目标地址动态转换关系
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式

Red-Giant(config-if)#**ip nat inside**	定义接口连接内部网络
Red-Giant(config)# **interface** *interface-type interface-number*	进入接口配置模式
Red-Giant(config-if)#**ip nat outside**	定义接口连接外部网络

5.6.5 配置特殊应用 NAT

特殊应用是指一些应用的有效载荷中包含有 IP 地址和端口,然后又试图使用这些内嵌的 IP 地址和端口号建立 TCP 或 UDP 会话。比如 FTP、DNS、SNMP、RealAudio、SIP、H323 应用以及一些游戏软件等。

目前版本的 RGNOS 软件 NAT，缺省情况下支持 FTP、DNS 应用,这些应用兼容在 RFC3027 中有规定，另外还支持腾讯 QQ 应用加速、帝国时代游戏以及 NetMeeting 等应用。

如果是内部网络主机做帝国时代游戏的服务器，为了方便配置，RGNOS 软件提供了一个专门的配置命令。要配置 NAT 支持内部网络主机做帝国时代游戏服务器，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip nat application dplay server** *server-local-address* **map** *server-global-address*	指定帝国时代服务器,供外部主机连接
Red-Giant(config)#**no ip nat application h323 server** *server-local-address* **map** *server-global-address*	取消配置

如果你知道帝国时代的服务端口(一般该端口号为 47624，最好根据实际端口号进行配置)，也可以直接配置静态 NAPT：

命令	作用
Red-Giant(config)#**ip nat inside source static tcp** *server-local-address* 47624 *server-global-address* 47624	指定帝国时代服务器,供外部主机连接
Red-Giant(config)#**no ip nat inside source static tcp** *server-local-address* 47624 *server-global-address* 47624	取消配置

5.6.6 调整地址转换超时时间

静态 NAT 转换是永久有效的，但动态 NAT 转换空闲一段时间后就会超时。要调整 NAT 地址转换超时时间，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip nat translation timeout** *seconds*	定义简单动态 NAT 转换超时时间，缺省 600 秒
Red-Giant(config)#**ip nat translation dns-timeout** *seconds*	定义 DNS 转换记录的超时时间，缺省 60 秒
Red-Giant(config)#**ip nat translation finrst-timeout** *seconds*	定义 TCP 连接 FIN 以及 RESET 后转换记录的超时时间，缺省 60 秒

Red-Giant(config)#**ip nat translation icmp-timeout** *seconds*	定义 ICMP 转换记录的超时时间，缺省 60 秒
Red-Giant(config)#**ip nat translation tcp-timeout** *seconds*	定义 TCP 连接转换记录的超时时间，缺省 600 秒
Red-Giant(config)#**ip nat translation udp-timeout** *seconds*	定义 UDP 连接转换记录的超时时间，缺省 300 秒

5.6.7 NAT 配置示例

本节提供了以下配置配置例子：

- 动态内部源地址转换示例
- 内部全局地址复用示例
- 重叠地址转换示例
- TCP 负载均衡示例

动态内部原地址转换示例。在以下配置中，本地全局地址从 NAT 地址池 net200 中分配，该地址池定义了地址范围为 200.168.12.2~200.168.12.100。只有内部源地址匹配访问列表 1 的数据包才会建立 NAT 转换记录。

```
!
interface FastEthernet0
 ip address 192.168.12.1 255.255.255.0
 ip nat inside
!
interface FastEthernet1
 ip address 200.168.12.1 255.255.255.0
 ip nat outside
!
ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
ip nat inside source list 1 pool net200
access-list 1 permit 192.168.12.0 0.0.0.255
```

通过显示 NAT 映射表，可以看到是否能够正确建立转换记录：

```
Red-Giant#sh ip nat translations verbose
Pro Inside global     Inside local      Outside local     Outside global
--- 200.168.12.2      192.168.12.2      ---               ---
create 00:00:42, use 00:00:33, left 00:09:26, flags: none
```

内部全局地址复用示例。内部全局地址复用，其实就是 NAPT。在定义地址池时写上 “ overload ” 参数就可以复用地址池中的全局地址了。在以下配置中，本地全局地址从 NAT 地址池 net200 中分配，该地址池只定义 200.168.12.200 一个 IP 地址，但允许复用。只有内部源地址匹配访问列表 1 的数据包才会建立该类型 NAT 转换记录。

```
!
interface FastEthernet0
 ip address 192.168.12.1 255.255.255.0
 ip nat inside
!
interface FastEthernet1
```

```
 ip address 200.168.12.1 255.255.255.0
 ip nat outside
!
ip nat pool net200 200.168.12.200 200.168.12.200 netmask 255.255.255.0
ip nat inside source list 1 pool net200
access-list 1 permit 192.168.12.0 0.0.0.255
```

通过显示 NAT 映射表，可以看到是否能够正确建立转换记录：

```
Red-Giant#show ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
   create 00:00:19, use 00:00:10, left 00:09:49, flags: extended
Red-Giant#
```

重叠地址转换示例。当内部网络地址与外部网络地址重叠时，外部重叠地址在内部网络上应该表现为不同的私有网络地址。在以下配置中，内部网络分配了非注册的 192.198.12.0/24 网络地址，外部网络已经分配了该地址，因此当内部网络通过域名方式访问外部重叠地址主机时，NAT 会将重叠地址转换为地址池 net172 中的地址，这样重叠地址的问题就解决了。以下配置，访问外部重叠地址主机时，只能通过主机域名，如果需要通过 IP 地址直接访问，就要配置外部源地址静态 NAT 映射。内部主机访问外部主机的映射方式采用动态 NAPT 方式。

```
!
interface FastEthernet0
 ip address 192.198.12.1 255.255.255.0
 ip nat inside
!
interface FastEthernet1
 ip address 200.198.12.1 255.255.255.0
 ip nat outside
!
!
ip nat pool net200 200.198.12.2 200.198.12.100 netmask 255.255.255.0
ip nat pool net172 172.16.198.2 172.16.198.100 netmask 255.255.255.0
ip nat inside source list 1 pool net200 overload
ip nat outside source list 1 pool net172
ip route 172.16.198.0 255.255.255.0 200.16.23.2
access-list 1 permit 192.198.12.0 0.0.0.255
!
```

通过显示 NAT 映射表，可以看到是否能够正确建立转换记录：

```
Red-Giant#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 200.168.12.2:1256 192.168.12.91:1256 200.168.168.11:53 200.168.168.11:53
tcp 200.168.12.2:1257 192.168.12.91:1257 172.16.198.2:23  192.168.12.91:23
--- ---                ---                172.16.198.2       192.168.12.91
Red-Giant#
```

在以上配置中，如果没有配置到 172.16.198.0/24 的静态路由，从内部接口接收到目标地址为该网络的数据包，路由器不能判断出来该数据将往哪个接口转发，导致通讯失败。所以当配置重叠地址时，必须配置静态路由或者在 outside 接口配置次 IP 地址，使得路由器知道地址转换以后该往哪个接口转发数据包。

TCP 负载均衡示例。在以下配置中，定义了一个虚拟主机地址，所有来自外部网络访问该虚拟主机的 TCP 连接，将被路由器分配到多台实际主机上，从而实现负载分流的目标。Realhosts 定义了实际主机地址池，访问列表 1 定义了虚拟主机地址。以下配置，只对 TCP 流量产生作用，对其它流量保持不变，除非有另外的 NAT 配置。

```
!
interface FastEthernet0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
interface FastEthernet1
 ip address 200.198.12.1 255.255.255.0
 ip nat outside
!
ip nat pool realhosts 10.10.10.2 10.10.10.3 netmask 255.255.255.0 type rotary
ip nat inside destination list 1 pool realhosts
access-list 1 permit 10.10.10.100
!
```

通过显示 NAT 映射表，可以看到是否能够正确建立转换记录：

```
Red-Giant#sh ip nat translations
Pro Inside global   Inside local    Outside local         Outside global
tcp 10.10.10.100:23 10.10.10.2:23  100.100.100.100:1178 100.100.100.100:1178
tcp 10.10.10.100:23 10.10.10.3:23  200.200.200.200:1024 200.200.200.200:1024
```

第六章 安装故障处理

6.1　电源故障排除

锐捷系列路由器可以根据前面板上的 POWER 指示灯来判断路由器电源系统是否出现故障。电源系统工作正常时，POWER 指示灯应保持常亮。如果电源指示灯 POWER 不亮时，请进行如下检查：

- 路由器电源开关是否打开
- 路由器供电电源开关是否打开
- 路由器电源线是否连接正确
- 路由器供电电源与路由器所要求的电源是否匹配

警告：

请不要带电插拔电源线，如果检查确认一切没有问题，电源 POWER 指示灯还是不亮，请与当地分销商或技术支持人员联系。

6.2　配置系统故障排除

路由器上电后，如果系统正常，在终端上将显示在第四章启动过程中所描述的信息。如果配置系统出现故障，终端上可能无显示或者显示乱码。

如果终端没有显示信息，请进行如下检查：

- 电源系统是否正常。
- 控制台口电缆是否正确连接

如果以上检查确认没有问题后，还是无法显示，很可能是配置电缆错误或者终端参数的设置错误，请调整终端的参数。

如果终端上出现乱码，可能是因为终端参数配置不匹配导致，请确认终端参数：波特率为 9600；数据位为 8；奇偶校验为无；停止位为 1； 流量控制为无；终端仿真为 VT100。

说明：

如果您的路由器控制台口参数已经被修改，则也可能导致终端不显示。

第七章 路由器的维护

7.1　ROM 监控模式维护与升级

7.1.1　ROM 监控模式简介

路由器软件包括 BootROM 启动软件和 RGNOS 路由器主体软件两种，两种软件运行在不同的模式下，BootROM 软件在路由器开机时，负责启动路由器，同时将路由器主体软件从 FLASH（闪速存储器）中读入到内存，启动完毕后，路由器便退出了 BootROM 软件，进入到正常运行模式，在正常运行模式下，便是 RGNOS 路由器主体软件在工作了，BootROM 软件也有自己的提示符和命令行接口，进入到 BootROM 提示符状态时，便称为 ROM 监控模式，在 ROM 监控模式下，可以完成路由器的 BootROM 升级，RGNOS 主体软件的升级，以及一些路由器的其他维护工作。

7.1.2　如何进入 ROM 监控模式

如果在 BootROM 软件启动时，无法在 FLASH 内找到合法的 RGNOS 主体软件映像时，便直接进入到 ROM 监控模式了。也可以采用手工进入，首先在路由器的 Console 口用标准 RS-232 线缆连接一台微机，并且在微机上运行终端仿真程序，在开机后的 3 秒内按**<Ctrl+Break>**，便进入了 ROM 监控模式了。

启动路由器，当出现

Start BOOTROM V1.9 build 1　（该提示版本不同，可能有所区别）

的时候，在 3 秒钟内按下 CTRL＋Break，出现以下提示：

boot:提示符

即进入 ROM 模式，在 boot:提示符下输入‘ ？ ’回车，便看到在 ROM 模式下可以执行的指令：

```
boot: ?
boot            boot up an external process
help            monitor builtin command help
reset           system reset
show-env        display the boot env-variables
show-log        display the log of factory test
save            write boot-rom env variable to FLASH
env-delete      unset a boot env-variable
xmodem          x/y modem download
tftp            tftpdown
boot:
```

说明：

要进入 ROM 监控模式，只能在 Console 口上连接终端的方式才可以，不支持其他异步口配置方式和 Telnet 客户端配置方式进入。

7.1.3 ROM 监控模式的升级功能

警告：

请不要随意进行路由器的软件升级，如确实有必要，最好在技术支持人员的指导下进行，另外在进行软件升级时，请注意确保所提供的升级文件和路由器的硬件版本匹配，同时千万不要将 BootROM 软件和路由器主体软件混淆，否则路由器无法启动。

7.1.3.1 ROM 监控模式下升级路由器主体软件

在 ROM 监控模式下，升级路由器主体软件的步骤如下：

选择用于升级的以太网口

锐捷系列路由器支持通过特定的以太网口对路由器的主体软件进行升级，对于 NBR100 系列路由器，选择 WAN 口。确定好以太口后，将该接口和一台有 TFTP 服务功能的微机（假定 IP 地址为 192.168.12.181）通过以太口连接，同时将路由器的配置口通过控制台线缆连接到一台微机的串口上（可以是同一台微机）。

在与路由器以太口连接的微机上运行 TFTP Server 程序，同时将升级路径指向放置升级文件（router.rom）的目录。

设置路由器的环境变量。

用 show-env 查看当前的路由器的环境变量，比如如下提示：

```
boot: show-env
PM=boot:
IP_ADDRESS=192.168.12.3
TFTP_SERVER=192.168.12.98
TFTP_FILE=router.rom
boot:
```

以上环境变量中，IP_ADDRESS 为路由器用于升级的以太口的 IP 地址，TFTP_SERVER 为运行 TFTP Server 的微机的 IP 地址，TFTP_FILE 为用于升级的路由器主体升级文件，这些环境变量根据具体的升级环境，需要进行重新设定，这些环境变量全部都为大写，同时在输入新值时，中间不能有空格。

运行 **tftp -c** 对路由器的主体软件进行升级

在 ROM 监控模式下升级路由器主体软件操作实例如下：

```
boot: show-env                                    ⇐查看当前环境变量
PM=boot:
TFTP_SERVER=192.168.12.98
IP_ADDRESS=192.168.12.3
TFTP_FILE=router.bin
boot: TFTP_SERVER=192.168.12.181                  ⇐修改 TFTP 服务器地址
boot: IP_ADDRESS=192.168.12.182                   ⇐修改路由器 IP 地址
boot: TFTP_FILE=router.rom                        ⇐修改升级文件名称
boot: show-env                                    ⇐确认修改后环境变量正确
PM=boot:
```

```
TFTP_SERVER=192.168.12.181
IP_ADDRESS=192.168.12.182
TFTP_FILE=router.rom
boot: tftp –c                                        ⇐开始升级路由器主体软件
 %Now Begin Download File router.bin From 192.168.12.181
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 %Mission Completion. FILELEN = 1796468
Now Init Flash...
Now Erase Flash ......
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEENow Copy Image To Flash (FileLen == 1796468)......
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK!]
You Must Reset or Power Cycle for New Config to Take Effect !
boot: reset                                ⇐升级成功，重启动路由器
```

注意：

使用 tftp –c 升级主体软件，请确保你所用软件为 rom 格式的文件，否则路由器无法启动。

如果你手上只有 bin 格式的升级软件，请先使用 tftp –r 下载软件，进入路由器后，在正常模式下升级主体软件。关于 tftp –r 下载软件的详细信息请参考“ ROM 监控模式网络下载执行功能 ”。

7.1.3.2 ROM 监控模式下升级路由器 BootROM 软件

在 ROM 监控模式下，升级路由器的 BootROM 监控软件的步骤和升级路由器主体软件的步骤基本相似，只是最后用于升级的指令的参数不同而已，**一定注意，升级文件不能弄错，否则路由器将彻底无法启动**，具体的升级步骤如下：

选择用于升级的以太网口

锐捷系列路由器支持通过特定的以太网口对路由器的 BootROM 软件进行升级，对于 NBR 系列路由器，选择 WAN 口。确定好以太口后，将该接口和一台有 TFTP 服务功能的微机（假定 IP 地址为 192.168.12.181）通过以太口连接，同时将路由器的配置口通过控制台线缆连接到一台微机的串口上（可以是同一台微机）。

在与以太口连接的微机上运行 TFTP Server 程序，同时将升级路径指向放置 BootRom 升级文件（bootrom.bin）的目录。

设置路由器的环境变量。

用 show-env 查看当前的路由器的环境变量，比如如下提示：

```
boot: show-env
PM=boot:
```

```
IP_ADDRESS=192.168.12.3
TFTP_SERVER=192.168.12.98
TFTP_FILE=router.bin
boot:
```

以上环境变量中，IP_ADDRESS 为路由器用于升级的以太口的 IP 地址，TFTP_SERVER 为运行 TFTP Server 的微机的 IP 地址，TFTP_FILE 为用于升级的文件名称，这些环境变量根据具体的升级环境，需要进行重新设定，这些变量全部都为大写，同时在输入新值时，中间不能有空格。

运行 **tftp -b** 对路由器的 BootROM 监控软件进行升级

在 ROM 监控模式下升级路由器 BootROM 监控软件的操作实例如下：

```
boot: show-env                                          ⇐查看当前环境变量
PM=boot:
TFTP_SERVER=192.168.12.98
IP_ADDRESS=192.168.12.3
TFTP_FILE=router.bin
boot: TFTP_SERVER=192.168.12.181                        ⇐修改 TFTP 服务器地址
boot: IP_ADDRESS=192.168.12.182                         ⇐修改路由器 IP 地址
boot: TFTP_FILE=bootrom.bin                             ⇐修改升级文件名称
boot: show-env                                          ⇐确认修改后环境变量正确
PM=boot:
TFTP_SERVER=192.168.12.181
IP_ADDRESS=192.168.12.182
TFTP_FILE=bootrom.bin
boot: tftp –b                                           ⇐开始升级 BootROM 软件
        %Now Begin Download File bootrom.bin From 192.168.12.181
        !!!!!!!!!!!!!!!!
        %Mission Completion. FILELEN = 207956
Download file ok! Erasing flash ...EEEEEEE  [OK]
Writing
flash ...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!![OK]
Update system boot rom OK! must restart!
boot:boot: reset                                        ⇐升级成功，重启动路由器
```

7.1.3.3 ROM 监控模式网络下载执行功能

对于手头路由器主体软件的映像文件，如果不能确定该映像文件是否正确，在功能上是否可以满足要求，不要随意的将该映像文件直接升级到路由器上，可以采用 RGNOS 提供的在 ROM 监控模式下，网络下载执行的功能，将映像文件从网络上下载到内存直接执行，来判断映像文件是否正确，功能是否可以满足需求，操作的步骤如下：

择用于下载的以太网口

对于 NBR100 系列路由器，选择 WAN 口。确定好以太口后，将该接口和一台有 TFTP 服务功能的微机（假定 IP 地址为 192.168.12.181）通过以太口连接，同时将路由器的配置口通过控制台线缆连接到一台微机的串口上（可以是同一台微机）。

与路由器以太口连接的微机上运行 TFTP Server 程序，同时将升级路径指向放置升级文件（router.bin）的目录。

设置路由器的环境变量。

用 show-env 查看当前的路由器的环境变量，比如如下提示：

```
boot: show-env
PM=boot:
IP_ADDRESS=192.168.12.3
TFTP_SERVER=192.168.12.98
TFTP_FILE=router.bin
boot:
```

以上环境变量中，IP_ADDRESS 为路由器用于升级的以太口的 IP 地址，TFTP_SERVER 为运行 TFTP Server 的微机的 IP 地址，TFTP_FILE 为用于升级的路由器主体升级文件，这些环境变量根据具体的升级环境，需要进行重新设定，这些环境变量全部都为大写，同时在输入新值时，中间不能有空格。

运行 **tftp –r** 下载执行对路由器主体软件

在 ROM 监控模式下下载执行路由器主体软件操作实例如下：

```
boot: show-env                                        ⇐查看当前环境变量
PM=boot:
TFTP_SERVER=192.168.12.98
IP_ADDRESS=192.168.12.3
TFTP_FILE=router.bin
boot: TFTP_SERVER=192.168.12.181                      ⇐修改 TFTP 服务器地址
boot: IP_ADDRESS=192.168.12.182                       ⇐修改路由器 IP 地址
boot: TFTP_FILE=router.bin                            ⇐修改升级文件名称
boot: show-env                                        ⇐确认修改后环境变量正确
PM=boot:
TFTP_SERVER=192.168.12.181
IP_ADDRESS=192.168.12.182
TFTP_FILE=router.bin
boot: tftp –r                                         ⇐下载执行路由器主体软件
        %Now Begin Download File router.bin From 192.168.12.181
        !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!
        %Mission Completion. FILELEN = 1821060

Image load complete! Please wait ...
Uncompress begin...
Uncompressing the image :
==================================================== [OK]
Red-Giant Operating System Software
RGNOS (tm) RELEASE SOFTWARE, Version 6.13(3)
Copyright (c) 1999-2002 by Start Network Technolgy co., Ltd.
Compiled Mon 02-Dec-02 14:04 by Markle

SUMSUNG K9F6408 ,Flash ID=ECE6
Start NBR100 (Samsung 4530(ARM7TDMI)) processor with 14336K/2048K bytes of memory
.
Processor board ID 00000062, with hardware revision 00000002
Controllers/Moduler cards list:

Samsung 4530 10/100M ethernet controller.
-----------------------------------------------
2 FastEthernet/IEEE 802.3 interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
```

```
Press RETURN to get started!

%CHANGED: Interface FastEthernet1, changed state to administratively down
%CHANGED: Interface FastEthernet2, changed state to administratively down
Red-Giant>
```

说明：

下载执行功能也用于将普通版升级到企业版，由于没有 rom 格式的主体软件，使用下载执行功能进入路由器正常模式，然后在正常模式下升级路由器主体软件。

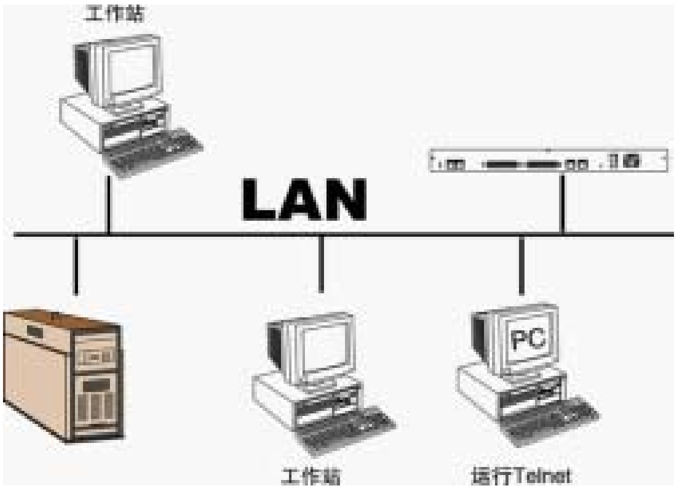
7.2　正常工作模式维护与升级

7.2.1　正常工作模式下路由器升级前准备

正常工作模式就是指路由器运行在正常工作状态下，在正常工作模式下，路由器可以完成利用 TFTP 服务器，升级路由器主体程序和模块上的微代码程序的功能；可以利用 TFTP 备份路由器的配置、设置路由器，所有这些功能都只用一个 COPY 命令来完成。

使用这些功能之前，必须先搭建一个合适升级环境，事先做好如下的准备：

路由器和用于升级路由器的微机在同一网络环境内，保证路由器和微机在网络上相通，搭建一个如下图所示的升级环境。



用 Telnet 配置模式对路由器进行远程升级

在微机上启动 TFTP Server。

给路由器对应接口配置 IP 地址，该 IP 地址不能和网络上的其他设备冲突，并且与 TFTP Server 微机可以相互通讯。

可以在路由器方先用 Ping 测试网络的连通性，如果能 Ping 通，说明使用正常工作模式下的维护功能的环境才能满足。

说明：

在正常工作模式下，对路由器的主体程序、模块上微代码程序进行升级时，可以采用任何的连接方式进入配置模式，可以在 Console 口进入，也可以通过异步口进入，还可以用 Telnet 的方式进入配置模式，都可以执行升级的命令，在升级路由器的主体程序时，不会影响路由器的正常运行，不过如果升级正在使用模块的微代码程序时，则会影响路由器的正常工作了，建议不要对正在工作的路由器进行升级。

7.2.2 正常工作模式下路由器主体程序的升级

做好上述的升级前的准备工作,并且将用于升级的路由器主体程序文件拷贝到 TFTP 服务器所指定的目录下，在路由器特权用户模式下执行如下命令：

Red-Giant#copy tftp flash

然后根据提示输入对应的参数。

正常工作模式下路由器主体程序的升级操作实例如下：

```
Red-Giant#copy tftp flash                                ⇐执行升级命令

System flash directory:
File  Length   Name
  1   1826800  router.bin
[1826864 bytes used, 6561744 available, 8388608 total]
                                                  ⇐输入 TFTP 服务器的 IP 地址
Address or name of remote host [255.255.255.255]? 192.168.12.181
Source file name? router.bin                      ⇐输入文件名称
Destination file name [router.bin]? myrouter.bin  ⇐输入保存在路由器上的文件名
Accessing file 'router.bin' on 192.168.12.181...
Loading router.bin .from 192.168.12.181 (via FastEthernet0): ! [OK]

Copy 'router.bin' from server
  as 'myrouter.bin' into Flash WITH erase? [yes/no]y
Erasing device...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Loading router.bin from 192.168.12.181 (via FastEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1826800/8388608 bytes]
Verifying checksum...  OK (0x9904)                        ⇐升级准确无误
Flash copy took 00:00:13 [hh:mm:ss]
```

7.3 应对密码遗失

用户忘记 NBR 路由器的密码时，可以采用如下的方法来解决：

1).准备一台运行仿真终端程序的 PC，推荐使用 Procomm 或 Windows Hyper Terminal(超级终端)；

2).将 PC 的串口和 NBR 路由器的控制台口用扁平控制台线缆连接好；

3).关机然后重启路由器，在超级终端上按 CTRL+Break 组合键(注意在加电之后迅即按下该组合键可能导致路由器被锁住，在这种情况下，需要重启路由器。需要说明的是终端仿真程序使用不同的按键组合来产生中断序列，最流行的两大终端仿真器是超级终端 和 Procomm，对于超级终端应同时按下 Ctrl+ Break 来产生中断序列，而 Procomm 则要同时按下 ALT+B 键。另外，密码修复工作只能在将超级终端连到路由器控制台端口的情况下才可被执行，这些步骤在路由器的辅助端口是行不通的)，然后路由器会进入 rom 监控模式，出现了 boot:的提示符。

4).在 boot:提示符下运行隐含命令 setup-reg，出现如下的选择菜单，

```
boot: setup-reg
  Configuration Summary
enabled are:
bypass the system configure file
console baud: 9600
do you wish to change the configuration? y/n  [n]:
```

在这里输入'*y*'，然后回车，系统会提示：

```
enable  "bypass the system configure file"? y/n  [n]:
```

在这里输入'y'，然后回车，接下去的全部直接回车，采用缺省的应答。最后路由器会提示：

```
You must reset or power cycle for new config to take effect
```

在 boot:提示符下输入 ***reset***，路由器会重启。这种情况下路由器重在启动时，将忽略 NV 内存中的配置信息，便不存在控制密码和使能密码了。路由器启动后直接回车，便直接进入路由器的命令提示符下。

```
Press RETURN to get started!
Router>enable
Router#
```

5).如果配置无关紧要，那么直接在特权层下运行 ***write***，然后 ***reboot*** 路由器便可以了；如果其中的配置还需要用到，那么可以在特权层下，执行命令 ***copy startup-configuration running-configuration*** 来完成这项任务，然后执行 ***config terminal***

命令进入全局配置模式，运行 ***enable secret 0*** *abcde*，这里的 “ abcde ” 便是新的密码了，完成之后可按下 ctrl + Z 组合键退出配置模式，键入 ***write*** 将新密码保存到 NV 内存中，然后重启路由器。

6).重启路由器，还是按照上面的步骤，进入到 rom 监控模式下，boot::提示符下输入 ***setup-reg*** 然后回车

```
boot: setup-reg
   Configuration Summary
enabled are:
bypass the system configure file
console baud: 9600
do you wish to change the configuration? y/n  [n]:
```

在这里输入'y'，然后回车，系统会提示：

```
disable  "bypass the system configure file"? y/n  [n]:
```

在这里输入’y’，然后回车，接下去的全部直接回车，采用缺省的应答。

7).在 boot:下运行 ***reset*** 重启路由器，到这一步，实现了修改密码的目的，现在路由器便可以采用新的密码来工作了。